Stefnur upplýsingatækni

HÁSKÓLINN
Á BIFRÖST

Efnisyfirlit

Yfirlit

Háskólinn á Bifröst setur stefnur um upplýsingatækni og notkun á gögnum, tölvum, tölvukerfum og hugbúnaði í eigu háskólans. Notkun á gögnum er í samræmi við skjalastefnu háskólans.

Stefnur um upplýsingatækni og verklagsreglur sem á þeim byggja er ætlað að auka öryggi og vernd gegn atvikum sem geta skaðað starfsemi skólans.

Virkar stefnur krefjast samstarfs og skuldbindingar allra sem koma að rekstri og starfi háskólans og það er á ábyrgð allra notenda að kynna sér og fylgja stefnum háskólans.

Stefnum háskólans um upplýsingatækni er fylgt eftir af upplýsingatæknisviði Háskólans á Bifröst og skulu þær endurskoðaðar eftir þörfum en að lágmarki á þriggja ára fresti.
Ef notendur brjóta gegn stefnum um upplýsingatækni mega þeir eiga von á viðurlögum.
Upplýsingatæknisvið hefur heimild til að loka á aðgang að gögnum og kerfum háskólans ef þörf krefur.

Undirskrift: …….. Dagsetning:…….

Yfirfarið á fundi í Háskólaráði 28. maí 2024

Gildir frá 1. ágúst 2024

Staðfest af rektor 28. maí 2024

Breytingasaga

Útgáfa 1	Dagsetning:	Upphafsstafir:

Skilgreiningar

Upplýsingatæknikerfi eru tölvur, netbúnaður, fjarskiptakerfi og hugbúnaður sem notaður er vegna starfsemi háskólans.

Gögn eru rafræn gögn og upplýsingar í eigu Háskólans á Bifröst á hvaða formi sem er. Rafrænum gögnum er safnað, viðhaldið og stjórnað í samræmi við skjalavistunaráætlun háskólans.

Upplýsingatækniauðlind eru gögn og upplýsingtæknikerfi í eigu háskólans.

Notandi (notendur) eru allir sem koma að rekstri og starfi háskólans hvort sem um er að ræða nemendur, starfsmenn, verktaka, þjónustuaðila hugbúnaðar, endurskoðendur, gesti og samstarfsaðila hafi þeir aðgang að upplýsingatækniauðlindum háskólans.

Netþjónn er skilgreindur sem netþjónn á innra neti háskólans.

Upplýsingar og gögn með takmarkaðan aðgang: Upplýsingar og gögn óháð sniði sem er safnað, þróað, viðhaldið eða stjórnað af eða fyrir hönd háskólans á upplýsingatæknikerfum háskólans og sem eru háð sérstakri vernd samkvæmt lögum eða reglum ríkisins eða samkvæmt gildandi samningum. Dæmi eru meðal annars, en eru ekki takmörkuð við, kennitölur, kreditkortanúmer, ökuskírteini, skrár nemenda, reglur um meðferð rannsóknar upplýsinga, fjárhagsgögn og útflutningsstýrð tæknigögn.

Öryggistengd atvik fela í sér en takmarkast ekki við;

- Að nálgast gögn eða búnað sem notandi skal ekki hafa aðgang að.
- Vírussýkingar eða innbrot í tölvu eða upplýsingatæknikerfi háskólans.
- Hvers konar vefveiði í gegnum tölvupóst eða til dæmis SMS.
- Truflanir á nettengingum teljast, en takmarkast ekki við, netþef, pingað flóð, pakkaskekkju, þjónustuneitun eða aðrar skaðlegar aðgerðir.

Hlutlaust svæði (DMZ, de-militarized zone) er sérhvert net sem er tengt við, en aðskilið frá, neti háskólans með eldvegg. Hlutlaust svæði er notað fyrir utanaðkomandi (Veraldarvef/samstarfsaðila, o.s.frv.) aðgang innan Háskólans á Bifröst, eða til að veita utanaðkomandi aðilum upplýsingar. Aðeins hlutlaus svæði sem tengjast internetinu falla undir gildissvið þessarar stefnu.

Traust tenging, beintenging utan umferðaræðar eða rásir með sterkri dulkóðun í samræmi við ásættanlega dulkóðunarstefnu. Ódulkóðaðar rásir verða að nota sterka notendavottun (einskiptislykilorð).

Ótryggt net er sérhvert net sem er aðskilið með eldvegg frá neti háskólans til að forðast truflanir á starfsemi vegna óreglulegrar netumferðar (rannsóknarstofunet), óviðkomandi

aðgangs (samstarfsnet, internetið o.s.frv.), eða eitthvað annað sem er auðkennt sem hugsanleg ógn við þessar upplýsingatækniauðlindir.

Ólöglegur hugbúnaður er hugbúnaður sem er dreift, notaður eða fenginn í trássi við höfundarréttarlög eða hugbúnaðarleyfi.

SSH (secure shell) er netsamskiptaaðferð sem gerir kleift að skiptast á gögnum með því að nota örugga rás milli tveggja nettækja.

IPSec (Internet Protocol Security) eru samskiptareglur til að tryggja Internet Protocol (IP) samskipti með því að auðkenna og dulkóða hvern IP pakka í gagnastraumi.

01 Almenn og viðunandi notkun

Tilgangur

Tilgangur þessarar stefnu er að tilgreina almenna og viðunandi notkun á upplýsingatæknikerfum og gögnum háskólans. Öll frávik frá settri stefnu stofna öryggi starfsemi háskólans í hættu m.a. vegna tölvuvírusa, árása á tölvunet og skaða á tölvuþjónustu.

Umsvif

Stefnan nær yfir alla notendur og upplýsingatækniauðlindir sem notaðar eru í þágu Háskólans á Bifröst eða í tengslum við umsvif háskólans.

Stefna

Undir engum kringumstæðum mega notendur framkvæma eða taka þátt í ólöglegu athæfi samkvæmt almennum lögum og reglum þjóðfélagsins, notandi upplýsingatæknikerfi háskólans.

Við hvers konar notkun á upplýsingatæknikerfum háskólans skulu notendur hafa í huga að þeir eru fulltrúar háskólans og ber að fara eftir siðareglum Háskólans á Bifröst.

Öll gögn Háskólans á Bifröst eru alfarið eign háskólans hvort sem þau eru geymd á tækjum skólans, í skýinu eða á tölvum, snjalltækjum og tölvukerfum í eigu eða leigu annara en háskólans.

Notendum er heimilt að nýta tæki sem þeim eru látin í té til takmarkaðra persónulegra nota. Háskólinn á Bifröst ber ekki ábyrgð á slíkri notkun eða persónulegum gögnum notenda og getur því ekki tryggt varðveislu þeirra, endurheimt eða öryggi. Háskólinn mælir með að persónuleg gögn séu vistuð í möppu sem ber skýrt heiti sem vísar til þess að um slík gögn sé að ræða s.s. „Persónulegt“.

Varðandi höfundarétt og afnotarétt á kennsluefni og rannsóknagögnum sem kennarar útbúa í störfum sínum fyrir Háskólann á Bifröst fer notkun þess eftir ákvæðum í samningi háskólans við viðkomandi starfsmann.

Tryggja skal að öll gögn háskólans séu varin samkvæmt reglum um gagnaöryggi og vistuð samkvæmt skjalastefnu Háskólans á Bifröst, með rafrænum og lagalegum hætti.

Notendur bera ábyrgð á því að tilkynna tap, stuld eða misnotkun á gögnum háskólans til yfirmanns, umsjónaraðila, kennara, skjalastjóra eða upplýsingatæknisviðs.

Notendur skulu meta ásættanlega notkun á upplýsingum og gögnum háskólans. Ef í vafa, skal ráðfæra sig við kennara, yfirmann, umsjónaraðila eða stjórnendur háskólans.

Sækja má og nota gögn Háskólans á Bifröst til að sinna starfi eða námi sem skyldi í samræmi við aðgangsstefnu háskólans.

Allar tölvur og snjalltæki í eigu háskólans skulu vera vernduð með skjáhvílu með lykilorði og hvíldartíma. Tölvur og snjalltæki skulu sett í hvíld eða slökkt á þeim þegar farið er frá þeim samanber stefnu um Ganga frá og loka tölvu.

Gæta skal sérstakrar varúðar þegar tölvupóstar eða skilaboð koma frá óþekktum aðilum. Notendur skulu varast að opna tölvupóst og viðhengi eða hlekki sem geta innihaldið eða vísað á spiliforrit eða beiðni um viðkvæmar upplýsingar.

Notendur skulu hafa samband við upplýsingatæknisvið hafi þeir grun um að hafa lent í vefveiðum eða öðrum netglæpum sem tengjast upplýsingatæknikerfum háskólans.

Keðju- og ruslpósta skal ekki áframsenda.

Öll lykilorð notenda og lykilorð á stjórnunar- og viðhaldsstigi skulu vera samkvæmt stefnu um lykilorð.

Aldrei skal auðkenna eða samþykkja auðkenningu sem þú hefur ekki stofnað til.

Notendur skulu setja fyrirvara sem segir að skoðanir og fullyrðingar eru þeirra eigin ef þeir senda tölvupóst frá tölvupóstfangi háskólans út fyrir starfsemi háskólans.

Umsjón og vöktun með tækjum, upplýsingatæknikerfum og netumferð mega aðeins ákveðnir starfsmenn Háskólans á Bifröst framkvæma, samkvæmt reglum er varða öryggi gagna og viðhald upplýsingatæknikerfa.

Við notkun hvers konar gagnageymslna svo sem skýjalausna, minnislykla og flakkara, bera notendur ábyrgð á að gagnageymslur séu verndaðar með viðeigandi öryggisráðstöfunum.

Ef þörf er á að aftengja eða hindra vírusvörn á tækjum háskólans vegna sérstakra ástæðna skal það gert í samráði við upplýsingatæknisvið. Setja skal vírusvörn á aftur eins fljótt og hægt er. Ekki má nota forrit sem geta dreift vírusum og spilliforritum meðan vírusvörn er niðri. Dæmi um slíkt eru tölvupóstar eða flutningur og deiling hugbúnaðar.

Eftirtalið eru bannað undir öllum venjulegum kringumstæðum. Starfsmenn geta haft undanþágu vegna starfa sinna og ábyrgðar svo sem net- og kerfisstjórar.

Neðan talið er ekki endanlegur listi um hvað ekki má, heldur setur ramma um hvaðeina athæfi sem telst “Það sem ekki má”.

- Brot á réttindum nokkurrar persónu eða fyrirtækis sem nýtur verndar höfundarréttar, viðskiptaréttar, einkaleyfis eða hugverks undir vernd almennra laga og réttar.
- Að nota hugbúnað á tölvum háskólans sem er ekki með fullt hugbúnaðarleyfi.
- Afritun af gögnum og hugbúnaði sem eru undir höfundarrétti og falla ekki undir samninga háskólans um afritun á höfundarvörðu efni vegna kennslu.
- Nota sértækan aðgang að gögnum, upplýsingatæknikerfum og neti háskólans til annars en verkefna sem tengjast starfsemi háskólans.

- Afritun af hugbúnaði, tækniupplýsingum, dulkóðun eða dulkóðunarhugbúnaði í trássi við lög og reglur er ólögleg. Ef í vafa skal hafa samband við yfirmann, tengilið við háskólann eða upplýsingatæknisvið.
- Setja skaðlegan hugbúnað inn á upplýsingatæknikerfi háskólans til dæmis tölvuvírusa, spilliforrit, trójuhesta og tölvupóstsprengjur.
- Deila aðgangsupplýsingum og lykilorði til að veita aðgang að upplýsingatækniauðlindum háskólans.
- Nota tæki og tól háskólans til að nálgast og nota hvers konar gögn sem brjóta í bága við lög um kynferðislega áreitni og fjandsamlegt framferði á vinnustað.
- Að nota tölvupóst háskólans til að bjóða og/eða selja hvers konar vörur eða þjónustu sem er ekki tengd starfsemi eða á vegum háskólans.
- Að valda öryggistengdum atvikum og truflunum á nettengingum.
- Framkvæma hvers konar vöktun á neti með þeim tilgangi að nálgast gögn ekki ætluð notanda nema sérstakt leyfi hefur verið gefið vegna lögmætrar vinnu.
- Misnotkun á auðkenningu að upplýsingatæknikerfum og gögnum.
- Að nota tælinet (Honeypot, honeynet, spam trap) og svipaða tækni.
- Breyta uppsetningu á notendareikningi eða tölvu í eigu háskólans.
- Notkun hvers konar forrits, forskriftar eða tölvuskipunar til að trufla aðgang eða notkun.
- Gefa upplýsingar um notendur háskólans til aðila utan háskólans.
- Senda óumbeðin skilaboð svo sem auglýsingar eða annan ruslpóst.
- Hvers kyns áreiti í gegnum tölvupóst, síma eða aðra samskiptamiðla. Hvort sem er val máls, magn eða tíðni.
- Óleyfileg notkun eða fölsun tölvupóstfangs.
- Beiðni um upplýsingar um notendur, ætluð til áreitni eða upplýsingasöfnunar utan starfsemi háskólans.
- Að senda tölvupósta frá tölvupóstfangi háskólans með upplýsingum um þjónustu sem er ekki í tengslum við starfsemi háskólans.
- Ekki eiga við og breyta uppsetningu og virkni vírusvarnaforrita sem eru uppsett á tölvum háskólans.

02 Upplýsingaöryggi

Tilgangur

Að tilgreina öryggiskröfur fyrir stjórnun og vernd upplýsinga og gagna háskólans.

Umsvif

Þessi stefna tekur til allra notenda og upplýsinga og gagna háskólans.

Stefna

Öryggiskröfur eru settar til verndar gegn hættum sem geta ógnað trúnaði, réttileika og aðgengi að gögnum sem og starfsemi og orðspori háskólans.

Háskólinn skuldbindur sig til að hámarka öryggi upplýsinga og gagna. Trúnaður, réttleiki og aðgengi gagna skal vera verndaður og tryggður. Háskólinn skal verja gögn með aðgangsstýringu, dulkóðun, afritun eða öðrum viðeigandi hætti, eftir því sem við á.

Styðjast skal við viðhlítandi staðla, lög og reglur til að tryggja öryggi upplýsinga og gagna. Þessi stefna miðar að því að fylgja viðmiðum ÍST ISO/IEC 27001 staðlinum – Stjórnunarkerfi um upplýsingaöryggi.

Notendur skulu fá fræðslu og þjálfun varðandi upplýsingaöryggi og skulu vernda gögn og upplýsingatæknikerfi gegn óheimiluðum aðgangi, breytingum eða tapi.

Notendur, hvort sem er um að ræða núverandi eða fyrrverandi, skulu ekki veita upplýsingar varðandi upplýsingar og gögn háskólans nema að fengnu samþykki ábyrgðaraðila.

Gögn nemenda við Háskólann á Bifröst sem vistuð eru á tölvukerfum háskólans, eru ekki skilgreind sem eign háskólans. Ef um ræðir öryggisatvik eða rökstuddan grun um brot á reglum háskólans, kann slíkt að fela í sér skoðun á innihaldi gagna nemenda í öryggisskyni. Slíkt verði þó eingöngu skoðað ef brýna nauðsyn ber til, verði þá farið eftir ferli við skoðun á tölvupósti eða gögnum nemenda. Komi til slíkrar skoðunar skal viðkomandi nemenda tilkynnt um hana fyrirfram, nema slíkt sé ómögulegt t.d. ef slík skoðun fer fram vegna yfirstandandi netárásar og skal þá nemenda tilkynnt um það svo fljótt sem auðið er.

Starfsfólk og verktakar Háskólans á Bifröst skulu athuga að allt efni og öll gögn vistuð á tölvukerfum háskólans, sem snúa að starfsemi háskólans, eru aðgengileg og teljast ekki einkamál. Öll gögn sem vistuð eru geta sætt skoðun á vegum háskólans ef þörf krefur, s.s. vegna viðbragða við atvikum s.s. netárásum eða vefveiðum, vegna lengri fjarveru notanda

sem krefst þess að nálgast þarf gögn hans til að tryggja hagsmuni Háskólans á Bifröst. Komi til slíkrar skoðunar skal viðkomandi notanda tilkynnt um hana fyrirfram, nema slíkt sé ómögulegt t.d. ef slík skoðun fer fram vegna yfirstandandi netárásar og skal þá notenda tilkynnt um það svo fljótt sem auðið er.

Gögn sem eru sérstaklega merkt sem einkamál og vistuð á tölvukerfum háskólans eru ekki rýnd nema vegna viðbragða við atvikum s.s. netárásum eða vefveiðum, ef brýn nauðsyn þykir. Þá skal ávallt upplýsa viðkomandi um skoðunina, ef þess er kostur og bjóða honum að vera viðstaddur. Ef ekki reynist unnt að láta vita fyrirfram um skoðunina skal upplýsa notanda strax og hægt er.

Upplýsingar og gögn skulu vera aðgengileg fyrir notendur samkvæmt þörfum og starfsemi háskólans.

Til að styðja stefnu um upplýsingaöryggi verða stefnur, verklagsreglur og leiðbeiningar fyrir háskólann að vera aðgengilegar á innri og ytri vef.

Samið skal um skilgreiningu á öryggiskröfum upplýsinga og gagna við alla birgja og aðra ytri aðila sem koma að starfi háskólans. Samningar og samþykktir skulu skjalfestir og framfylgt samkvæmt stefnu. Sem hluti af verklagi hvers verkefnis skulu sérstakar öryggisþarfir fyrir ný eða breytt kerfi eða þjónustu skilgreind.

Háskólinn skal tryggja að allt starfsfólk sem tekur þátt í upplýsingaöryggi sé hæft til að sinna hlutverki sínu með menntun og þjálfun. Þjálfunarkröfur skulu vera skilgreindar til að tryggja að viðeigandi færni sé til staðar fyrir áframhaldandi starfsemi.

Stöðugt skal leitast við að bæta upplýsingöryggi og reglulega skal framkvæma áhættumat og innri eða ytri úttektir til þess að greina áhættu og ógnir, bæta veikleika og auka upplýsingaöryggi.

Öll öryggisatvik skal tilkynna samkvæmt stefnu 03 Tilkynning og meðferð öryggistengdra atvika.

Háskólinn skal gera viðlagaáætlun til að vernda starfsemi sína og lágmarka mögulegan skaða vegna öryggisatvika (*Business continuity*).

03 Tilkynning og meðferð öryggistengdra atvika

Tilgangur

Þessi stefna tilgreinir hvernig bregðast skuli við öryggistengdum atburðum tengdum upplýsingatækni og hvernig skuli tilkynna og tryggja skilvirkar og skjótar aðgerðir, sem og skráningu öryggistengdra atvika.

Umsvif

Stefnan varðar alla notendur og öryggistengd atvik sem koma upp á upplýsingatæknikerfum háskólans.

Stefna

Öryggistengd atvik fela í sér en takmarkast ekki við;

- Að nálgast gögn eða búnað sem notandi skal ekki hafa aðgang að.
- Vírussýkingar eða innbrot í tölvu eða upplýsingatæknikerfi skólans.
- Hvers konar vefveiði í gegnum tölvupóst eða til dæmis SMS.
- Truflanir á nettengingum teljast, en takmarkast ekki við, netþef, pingað flóð, pakkaskekkju, þjónustuneitun eða aðrar skaðlegar aðgerðir.

Allir notendur skulu tilkynna öryggistengd atvik sem koma upp á tölvukerfum háskólans tafarlaust til upplýsingatæknisviðs og yfirmanns eða tengiliðar við háskólann.

Upplýsingatæknisvið ásamt yfirmanni eða tengilið, eftir því sem við á skulu greina eðli atviks og bregðast við samstundis til að takmarka hugsanlegt tjón.

Upplýsingatæknisvið skal flokka öryggistengd atvik eftir alvarleika þeirra og forgangsraða aðgerðum. Upplýsingatæknisvið skal framkvæma greiningu á öryggistengdu atviki, skrásetja orsakir og viðbrögð við atvikinu.

Ef atvik er talið alvarlegt og hefur valdið tjóni skal frekari rannsókn fara fram.

Rannsóknarteymi skal skipað af rektor háskólans og skal það gera samskiptaáætlun. Samskiptaáætlun skal taka til innri og ytri hagsmunaaðila eftir því sem við á og leita skal lögfræðiráðgjafar ef bregðast þarf við hugsanlegum lagalegum afleiðingum atviks. Varði atvikið persónuupplýsingar skal tilkynna það persónuverndarfulltrúa og eftir atvikum skal öryggisbrestur tilkynntur til Persónuverndar innan 72 klukkustunda frá því að vart varð við slíkan öryggisbrest.

Niðurstöður aðgerða vegna öryggisatvika skulu notaðar til að auka öryggi háskólans.

04 Lykilorð

Tilgangur

Stefnan setur reglur um aðgangsstýringu og smíði, meðhöndlun og vernd lykilorða.

Umsvif

Stefnan nær yfir alla notendur sem fá aðgang að upplýsingatækniauðlindum háskólans.

Stefna

Gögn og upplýsingatæknikerfi háskólans skulu vera með aðgangsstýringu sem krefst notkunar á sterkum lykilorðum. Vísað er til leiðbeininga hér fyrir neðan um samsetningu sterkra lykilorða

Háskólinn notar fjölþátta auðkenningu og aðgangur að viðkvæmum upplýsingatækniauðlindum skal ávallt varinn með fjölþátta auðkenningu. Notendur skulu skrá sig og nota fjölþátta auðkenningu þar sem við á.

Notendur sem geyma eða nota gögn háskólans á einkatölvum og snjalltækjum skulu verja þau tæki samkvæmt þessari stefnu. Athuga skal að auðkenning með aðferðum lífkenna í stað lykilorða á einkatækjum er leyft samkvæmt stefnu þessari og telst mæta lágmarkskröfu um öryggi gagna og upplýsingatæknikerfa háskólans.

Lykilorð eru trúnaðarupplýsingar og skulu ekki vera skráð á ótryggum stöðum.

Lykilorðum skal ekki deila með öðrum og aldrei skal deila lykilorði í tölvupósti eða á samskiptamiðli.

Háskólinn hvetur notendur til að nýta sér tækni til að geyma, stjórna og smíða sterk lykilorð. Upplýsingatæknisvið mælir með viðurkenndri tækni fyrir stjórnun lykilorða.

Notendur skulu nota sterk lykilorði sem veita lágmarks vörn gegn broti á aðgangi. Vísað er til leiðbeininga hér fyrir neðan um samsetningu sterkra lykilorða

Notendur skulu ekki nota sama lykilorð fyrir mismunandi aðgengi að upplýsingtækniauðlindum og ekki endurnota lykilorð.

Notandi með ítarlegt aðgengi skal ráðfæra sig við upplýsingatæknisvið um hvort rétt sé að hafa fleiri en einn aðgang og lykilorð til að skilja á milli venjulegrar almennrar notkunar og annarrar notkunar. Net- kerfis- og tækjastjórnendur með aukið aðgengi og ofurréttindi skulu hafa aðskilinn aðgang og lykilorð fyrir mismunandi tæki og kerfi og skulu lykilorð fyrir nauðsynleg tæki og gögn vera skráð í gegnum viðurkennt umsjónarkerfi fyrir lykilorð til öryggis ef kemur til áfalla.

<u>Almennar leiðbeiningar um samsetningu og meðferð lykilorða</u>

Varasamt er að nota þekkta hluti, fólk og minningar við samsetningu lykilorða og varast að einbeita sér að þægindum við innsetningu lykilorða því það skapar hættu á misnotkun aðila sem kynnir sér fjölskyldu og persónulega hætti starfsmanna. Dæmi um lykilorð sem ekki skal nota

- Orð úr orðabók, hvaða tungumál sem er.
- Nafn fjölskyldumeðlims, gæludýrs, samstarfsmanna, eða söguhetjur kvikmynda eða bóka.
- Tölvuhugtök, vefsíður, tölvuskipanir og annað tengt.
- Samsetningar úr nöfnum, bifbifrost sem mundi vera afbrigði af Bifröst, h-dalshnjukur sem væri breyting úr Hvannadalshnjúk.
- Afmælisdagar, heimilisföng, símanúmer og aðrar persónulegar upplýsingar.
- Stafa eða tölustafa mynstur, aaabbbaaa, 123454321, qwerty, zxcvfdsa.
- Hvaðeina að ofan stafað afturábak, tsorfib.
- Hvaðeina að ofan með tölustaf fyrir framan eða aftan. bifrost1, 1bifrost.
- Lykilorð skulu vera minnst 10 tákn samsett af bókstöfum háum og lágum, tölustöfum og táknum. Dæmi um notkun sem mælt er með ,
- Bæði háir og lágir stafir, a-z, A-Z.
- Tölur og tákn af lyklaborði, 0-9,!@#$ %^&*()_+|~-=\`{}[]:";'<>?,./) .
- Eru ekki orð eða slang úr neinu máli.
- Eru ekki persónulegar upplýsingar eða minningar.

Þar sem erfitt er að muna slíkar samsetningar þá er mælt með að starfsmenn finni sér aðferðir sem henta til að muna. Að nota setningar eða titla til að búa til lykilorð sem nýtist til að muna, svo sem ‘allir fyrir einn er alltaf best fyrir alla sem skipta máli’ Gæti skrifast sem @F1e@bF@ssm sem fullnægir kröfu um sérstafi, hástafi, tölustafi og lágstafi, athuga að hér er @ notað fyrir a og er Hástafurinn F notaður allstaðar þar sem f kemur fyrir. Í dag eru löng og einfaldari lykilorð talin sterkari en til dæmis flókin lykilorð með fáum táknum þar sem til dæmis fólk gæti átt erfitt með að muna mörg flókin lykilorð en getur sett saman löng einfaldari lykilorð.

Ekki skal skrifa niður lykilorð þar sem hægt er að ná til þeirra . Handskrifað eða prentað eða í gegnum vef og snjalltæki.

Upplýsingatæknisvið setur verklagsreglur um stýringu lykilorða og veita notendum aðstoð, upplýsingar og þjálfum eftir þörfum.

05 Aðgangsstefna

Tilgangur

Tilgangur aðgangsstefnu Háskólans á Bifröst er að auka og vernda öryggi gagna og upplýsingatæknikerfa háskólans.

Umsvif

Þessi stefna gildir fyrir allar notendur og upplýsingatækniauðlindir háskólans.

Stefna

Umsjón með gögnum og aðgangi að þeim skal skilgreind með hliðsjón af eðli gagna og tilgangi og skjalastefnu háskólans.

Umsjónaraðilar og eigendur gagna skulu alfarið stjórna aðgangi að gögnum í þeirra umsjá, með hliðsjón af gildandi lögum og reglum, svo sem persónuverndarlögum.

Skilgreina skal og skrá viðkvæmni gagna og hvort beitt sé flokkaður aðgangur ákveðinna hópa eða hvort er beitt persónubundnum aðgangi.

Aðgangur að gögnum og upplýsingatæknikerfum skal eingöngu vera veittur ef sannarleg þörf er á aðgangi til að sinna störfum. Skilgreina skal hlutverk notanda og aðgangur skal vera takmarkaður sem því svarar.

Aðgangur að gögnum og upplýsingatæknikerfum skal vera heimilaður af yfirmanni eða umsjónaraðila. Upplýsingatæknisvið veitir aðstoð varðandi stýringu aðgangs með tilliti til notkunarþarfa og trúnaðar eins og við á.

Ætlast má til að umsjónaraðilar gagna og upplýsingatæknikerfa geta nálgast tímasetningu og notendaupplýsingar allra þeirra sem hafa aðgang að kerfum Háskólans á Bifröst. Yfirmenn eiga að bera ábyrgð á að starfsmenn séu með viðeignadi tímasettan aðgang. Notandi skal hafa samþykkt allar leiðbeiningar hvað varðar aðgang og notkun á gögnum og upplýsingatæknikerfum háskólans.

Upplýsingatæknisvið veitir umsjónaraðilum gagna og upplýsingatæknikerfa tæknilega aðstoð en upplýsingatæknisvið veitir ekki aðgang án samþykkis yfirmanns og/eða umsjónaraðila.

Reglulega skal endurskoða aðgangs réttindi til að tryggja að þau endurspegli þörf sem svarar starfi og loka skal aðgangi að gögnum og upplýsingatæknikerfum í tengslum við starfslok eða starfsbreytingu.

Tölvur háskólans eru afhentar starfsfólki og eru settar upp með nauðsynlegum öryggisstillingum til verndar gegn tölvuvírusum, og annarri rafrænni óværu. Starfsfólk skal ekki hafa aðgang að stillingum og stjórnkerfi nema nauðsyn beri til og skal skrá þau tilvik.

Upplýsingatæknisvið skal skrá aðgang að neti og netþjónum með áherslu á að starfsfólk hafi aðgang að þeim tækjum og þjónustu sem þarf til að sinna sínum störfum. Einnig skal hafa örugga bakhjarla með aðgang að mikilvægum upplýsingatæknikerfum, tækjum og þjónustu til að viðhalda getu til viðhalds og viðgerða. Þar sem við verður komið skal rafrænt öryggiskerfi sem skráir aðgang vera notað til veita aðgang að tölvukerfum og tækjum í húsnæði háskólans.

Umsjónaraðilar gagna og upplýsingatæknikerfa skulu tryggja nauðsynlega þjálfun áður en aðgangur er veittur.

Við starfslok skal:

- Tímanlega loka á aðgang að upplýsingakerfum og gögnum.
- Endurheimta öryggislykla og kort eftir því sem við á.
- Endurheimt tölvu og tækja sem tryggir öryggi gagna og einnig að allar persónulegar upplýsingar eru fjarlægðar.
- Tryggja aðgang að upplýsingum, gögnum og upplýsingatæknikerfum sem áður var stjórnað af einstaklingi.
- Upplýsa notendaumhverfi um breytingu á ábyrgð.

Við flutning í starfi

- Skoða og staðfesta áframhaldandi þörf fyrir núverandi aðgangsheimildir að upplýsingakerfum og gögnum þegar einstaklingum er fluttur í starfi.
- Breyttu aðgangsheimild eftir þörfum til að samsvara breytingum á rekstrarþörf vegna flutnings í starfi og umsjónaraðilar kerfa og gagna skulu tryggja nauðsynlega þjálfun.
- Upplýsa notendaumhverfi um breytingu á hlutverki í starfi.

Vegna aðgangs verktaka og gesta skulu umsjónaraðilar gagna og upplýsingatæknikerfa

- Skjalfesta öryggiskröfur, þar með talið öryggishlutverk og ábyrgð fyrir utanaðkomandi.
- Tryggja að utanaðkomandi hlíti öryggisstefnu og verklagsreglum háskólans.
- Tryggja að þjónustuveitendur upplýsi um hvers kyns flutning í starfi eða starfslok þjónustuaðila.

06 Notkun á fartölvum

Tilgangur

Að tryggja öryggi upplýsinga og gagna háskólans og ábyrga notkun á fartölvum háskólans.

Umsvif

Þessi stefna gildir um alla notendur sem fá úthlutaða fartölvu frá háskólanum.

Stefna

Fartölvur sem háskólinn úthlutar notendum til að sinna stöfum sínum eru eign háskólans.

Notendur skulu ekki deila né afhenda öðrum fartölvu sem þeir fá úthlutaða.

Notendur eru ábyrgir fyrir öryggi og viðeigandi notkun á fartölvum sem þeir fá frá háskólanum.

Allar skemmdir, tap eða þjófnaður á fartölvu skal tilkynna til yfirmanns eða umsjónaraðila og upplýsingatæknisviðs. Notendur skulu tilkynna upplýsingatæknisviði um tæknivandamál og öryggistengd atvik sem tengjast fartölvum.

Notendur skulu skila fartölvu til upplýsingatæknisviðs vegna starfloka eða ef þeir fá úthlutaða nýja fartölvu.

Notendum er heimilt að nýta fartölvur sem þeim eru látin í té til takmarkaðra persónulegra nota. Háskólinn á Bifröst ber ekki ábyrgð á persónulegum gögnum og getur því ekki tryggt varðveislu þeirra, endurheimt eða öryggi.

Ekki skal nota fartölvur háskólans við hverskonar ólöglegt athæfi og ekki má skerða öryggi fartölva háskólans á nokkurn hátt, svo sem:

- Niðurhal og/eða uppsetning á ólöglegum hugbúnaði eða miðli.
- Uppsetning og uppfærslur á hugbúnaði skulu vera samþykktar af upplýsingatæknisviði.
- Breytingar á aðgangi, réttindum eða öryggisheimildum á fartölvu til að sniðganga vernd háskólans á vélbúnaði eða hugbúnaði.
- Ekki skal fjarlægja eða slökkva á spilli- og vírusvörnum uppsettum á öllum fartölvum háskólans.

Forðast skal að vista gögn og upplýsingar sem innihalda viðkvæmar upplýsingar á harða drifinu á fartölvum til að koma í veg fyrir tap eða brot á öryggi eða trúnaði ef fartölvan týnist eða er stolið.

Notendur sem þurfa að hafa viðkvæmar upplýsingar og gögn á fartölvum sínum, skulu ráðfæra sig við skjalastjóra og upplýsingatæknisvið um aðferðir til að auka öryggi upplýsinga og gagna.

Starfsmenn eru hvattir til að koma með allar fyrirspurnir um öryggisheimildir og takmarkanir til skjalastjóra og upplýsingatæknisviðs háskólans.

07 Vírusvarnarstefna

Tilgangur

Að setja kröfur sem allar tölvur Háskólans á Bifröst verða að uppfylla til að tryggja skilvirka skynjun og öflugar forvarnir gegn tölvuvírusum.

Umsvif

Stefna þessi nær til allra tölva háskólans, svo sem borðtölva, ferðatölva, allra tölvuþjóna og hvers kyns tækja í netþjónaherbergi, fundarherbergjum og öðrum rýmum háskólans.

Stefna

Allar tölvur Háskólans á Bifröst skulu hafa uppsetta vírusvörn til að tryggja gögn og upplýsingar bæði á tölvunum sjálfum sem og öðrum tölvum tengdum innan tölvukerfa háskólans. Einnig skulu önnur tæki eins og snjalltæki sem notuð eru til að vinna með og sækja gögn og upplýsingar háskólans vera varin með vírusvarnarforritum.

Vírusvarnir taka einnig til fræðslu og tilurð ferla til að varna gegn spilliforritum og vírusum sem koma til með öðrum leiðum eins og til dæmis í gegnum tölvupósta og USB flakkara.

Öll vírusvarnaforrit skulu uppfærð reglulega til að viðhalda varnargetu.

Ef að tölva eða tæki smitast af tölvuvírus eða spilliforriti, skal tölvan einangruð og skal ekki tengjast kerfum háskólans fyrr en hún hefur verið hreinsuð og vottuð.

Upplýsingatæknisvið skal vinna eftir verklagsreglum i sem tryggja að vírusvarnir séu uppfærðar reglulega og tölvur og tæki starfi í sem bestu ástandi.

Óleyfilegt er að búa til eða dreifa vírusum eða spilliforritum á tölvum og á tölvukerfum háskólans.

Fylgja skal leiðbeiningum og samþykktum verklagsreglum útgefnum af upplýsingatæknisviði um aðgerðir til varnar vírusum og spilliforritum.

Einkatölvur, minnislyklar, flakkarar og snjalltæki sem notuð eru við vinnu eða aðgengi að gögnum og upplýsingum háskólans skulu varin af vírusvarnarforritum og það er á ábyrgð eiganda að þeim sé viðhaldið og þau uppfærð reglulega.

08 Gagnageymslur

Tilgangur

Að tryggja örugga, áreiðanlega og ábyrga notkun á gagnageymslum eins og flökkurum, þumaldrifum, fartölvum og snjalltækjum.

Umsvif

Þessi stefna gildir um fartölvur, farsíma, snjalltæki og gagnageymslur sem eru notaðar til að meðhöndla gögn og upplýsingar háskólans óháð því hvert er eignahald tækis. Mikilvægt að hafa í huga er að þetta er ekki stefna um skjalvistun, heldur einungis um tæknibúnaðinn sem er notaður.

Stefna

Gögn og upplýsingar sem innihalda viðkvæmar upplýsingar á ekki að geyma á fartölvum, farsímum og öðrum geymslulausnum til að koma í veg fyrir tap eða brot á öryggi eða trúnaði ef tæki týnist eða er stolið.

Notendur sem þurfa að hafa viðkvæmar upplýsingar og gögn á geymslulausnum, skulu ráðfæra sig við skjalastjóra og upplýsingatæknisvið um aðferðir til að auka öryggi upplýsinga og gagna.

Allar fartölvur og gagnageymslur sem fá aðgang að innra neti Háskólans á Bifröst og/eða geyma viðkvæm gögn og upplýsingar, skulu vera í samræmi við reglur og staðla um upplýsingaöryggi háskólans.

Notendur bera ábyrgð á því að viðhalda geymslulausnum og gæta þess að þær séu öruggar og verndaðar.

Notendur skulu tilkynna til upplýsingatæknisviðs um mögulega öryggisbresti eða vandamál á geymslulausnum.

Viðkvæm gögn, sem geymd eru í fartölvum og geymslutækjum verða að vera varin með sterku lykilorði samanber stefnu um lykilorð.

Ekki skal dreifa eða senda gögn með takmarkað aðgengi frá Háskólanum á Bifröst til geymslu á, eða fá aðgang í gegnum, tæki sem uppfylla ekki þessar kröfur.

Starfsmenn eru hvattir til að koma með allar fyrirspurnir um öryggisheimildir og takmarkanir til skjalastjóra og upplýsingatæknisviðs háskólans.

09 Fjaraðgangur

Tilgangur

Stefnan skilgreinir hvernig fjaraðgangi að gögnum og innri og ytri upplýsingatæknikerfum háskólans er stjórnað til að koma í veg fyrir óleyfilega notkun og auka öryggi og heilindi gagna og upplýsingatæknikerfa.

Umsvif

Þessi stefna gildir um allar aðferðir sem háskólinn beitir til að veita fjaraðgang að upplýsingatæknikerfum og notendur sem stjórna og nýta sér þann aðgang. Stefnan nær yfir aðgang að kerfum og gögnum hvort sem þau eru hýst hjá háskólanum eða hjá ytri þjónustuaðilum.

Stefna

Fjaraðgangur að upplýsingatækniauðlindum háskólans skal ávallt metinn með tilliti til öryggis.

Háskólinn mun aðeins leyfa aðgang að upplýsingatækniauðlindum á innra neti háskólans í gegnum VPN eða aðra viðurkennda þjónustu og aðeins ef nauðsynleg þörf er á tengingu. Upplýsingatæknisvið verður að samþykkja slíkan aðgang og skal skrásetja og innleiða stýringar fyrir allar fjaraðgangsaðferðir að innra neti háskólans.

Fjaraðgangsaðferðir verða að nota viðeigandi öryggistækni til að tryggja fjartengingu, auk þess að koma í veg fyrir óviðkomandi aðgang og misnotkun á gögnum.

Notendur skulu nota fjölþátta auðkenningu til að tengjast kerfum á innra neti háskólans og er eindregið mælt með notkun á fjölþátta auðkenningu hvar sem ytri þjónusta styður hana.

Aðgangur að upplýsingatæknikerfum frá ytri þjónustuaðilum skal vera í samræmi við auðkenningar- og öryggiskröfur sem tilgreindar eru af þjónustuaðila.

Notendur skulu tilkynna mögulega öryggisbresti eða vandamál vegnar fjartengingar til upplýsingatæknisviðs.

Notendur bera ábyrgð á að vernda fjaraðgangsaðferðir, tæki og skilríki sem þeim er úthlutað. Notendur skulu viðhalda öryggi tölva og tækja sem notuð eru til að fá aðgang að upplýsingatæknikerfum háskólans.

Upplýsingatæknisvið ber ábyrgð á eftirliti með fjaraðgangsaðferðum og vöktun á netumferð til að koma í veg fyrir óleyfilega notkun og skal grípa til viðeigandi aðgerða vegna öryggisbresta eða óleyfilegrar notkunar Aðgerðir geta falið í sér eftirlit með netumferð notenda í öryggisskyni en þó eingöngu ef nauðsyn ber til s.s. vegna öryggisatviks eða rökstudds gruns um brot á reglum. Verður þá farið eftir verklagsreglum við skoðun á tölvupósti eða gögnum notenda. Ytri þjónustuaðilar skulu hafa eftirlit með fjaraðgangi og geta veitt háskólanum upplýsingar varðandi fjaraðgang sé farið fram á það.

10 Ganga frá og loka tölvu

Tilgangur

Að setja stefnu um hvernig skal skilið við og gengið frá tölvum háskólans í lengri eða skemmri tíma. Skýr stefna dregur úr hættu á óviðeigandi aðgangi, tapi eða skemmdum á upplýsingum og gögnum háskólans.

Umsvif

Þessi stefna tekur til alla notendur sem fá úthlutaða tölvu eða nota tölvu frá Háskólanum á Bifröst.

Stefna

Notendur skulu vernda allar upplýsingar og gögn sem þeir hafa aðgang að.

Aðgangur að tölvum skal vera varinn með aðgangsstýringu.

Notendur skulu skrá sig út af tölvum eða setja tölvu í svefn þegar þeir ganga frá tölvum.

Skjávörn skal vera sett upp á tölvum háskólans og vera stillt þannig að hún virkjast sjálfkrafa eftir ákveðinn tíma og tölva lokast. Notandi skal þurfa að auðkenna sig til þess að opna tölvuna aftur.

Tölvuskjár ætti að snúa frá sjónarhorni óviðkomandi eins og kostur er.

11 Netöryggisstefna

Tilgangur

Að tryggja örugga og viðeigandi notkun og stjórnun á netkerfi háskólans.

Umfang

Þessi stefna á við um alla notendur og netkerfi háskólans.

Stefna

Netkerfi háskólans er sett upp fyrir starfsemi háskólans og notendur skulu forðast persónulega notkun sem gæti haft neikvæð áhrif á afkastagetu netsins.

Notendur skulu ekki nota netkerfi háskólans til þess að taka þátt í ólöglegu athæfi eða athæfi sem brýtur í bága við reglur háskólans.

Aðgangur að netkerfi háskólans skal miðast regluna um við minnstu mögulegu réttindi og tryggja skal að notendur hafi einungis þann aðgang sem nauðsynlegur er til að sinna störfum sínum.

Nauðsynlegt er að auðkenna sig inn á netkerfi háskólans og fjölþátta auðkenningar (MFA) er krafist þar sem við á.

Nota skal eldveggi, vírusvarnarforrit, innbrotsskynjun og aðrar öryggisráðstafanir til að vernda netkerfi háskólans fyrir ytri og innri ógnum.

Öll viðkvæm gögn sem send eru um netið skulu vera dulkóðuð.

Hugbúnaður og vélbúnaður fyrir netkerfi skal uppfærður reglulega með öryggisuppfærslum og framkvæma skal reglulegt viðhald á honum sem tryggir afköst og öryggi.

Reglulega skal taka öryggisafrit af stillingum og gögnum er varða netkerfi sem tryggir aðgengi og samfellu í rekstri ef atvik koma upp.

Vélbúnað fyrir netkerfi skal staðsetja í umhverfi þar sem hægt er að stýra aðgangi. Óviðkomandi skal ekki hafa aðgang að vélbúnaði háskólans og aldrei skal skilja við tæki sem eru óvarin eða eftirlitslaus.

Til þess að tryggja upplýsingaöryggi og svo hægt sé að bregðast við öryggisatvikum skal vakta netumferð og skrá upplýsingar um netaðgang og virkni. Við vöktun netkerfis verða til upplýsingar um netnotkun einstaklinga. Slíkar upplýsingar er eingöngu heimilt að skoða ef nauðsyn ber til og skal tilkynna einstaklingi um slíka skoðun fyrirfram, nema slíkt sé ómögulegt t.d. ef slík skoðun fer fram vegna yfirstandandi netárásar og skal þá notendum tilkynnt um það svo fljótt sem auðið er.

Upplýsingatæknisvið skal gera áætlun til að draga úr áhættu vegna netárása og tryggja öryggi gagna og upplýsingatæknikerfa háskólans og skal hún endurskoðuð reglulega.

Notendur skulu tilkynna öll öryggisatvik eða grun um öryggisatvik til upplýsingatæknisviðs.

Hverskonar snuðrun/þefun (e. sniffing) á neti háskólans er ekki leyfileg.

Háskólinn skal stuðla að stöðugum umbótum og þjálfun starfsmanna hvað varðar netöryggi

12 Tölvupóstur

Tilgangur

Stefna þessi setur reglur um notkun tölvupósts með tölvupóstfangi Háskólans á Bifröst (@bifrost.is).

Umsvif

Allir notendur tölvupóstfangs háskólans.

Stefna

Tölvupóst skal nota til samskipta á milli notenda og samskipta við þá sem koma að starfsemi háskólans. Forðast skal að nota tölvupóst Háskólans á Bifröst fyrir einkasamskipti. Notendur skulu nota örugg lykilorð fyrir aðgang að tölvupóstkerfi háskólans samkvæmt stefnu um sterk lykilorð og skulu ekki deila því lykilorði með óviðkomandi.

Notendur skulu ekki nota tölvupóst háskólans til að miðla persónuupplýsingum.

Notendur skulu meta efni tölvupóst sem þeir senda og ef trúnaðarmál, persónuupplýsingar eða til dæmis efni sem tengjast fjármálakerfum háskólans er um að ræða verður að senda gögnin á öruggan hátt með viðeigandi leynd. Valmöguleikar í tölvupóstkerfi skulu nýttir til að verja slíkar upplýsingar.

Tölvupóst má ekki nota til að senda eða dreifa nokkurskonar truflandi eða særandi skilaboðum, svo sem athugasemdum um kynþátt, kyn, fötlun, aldur, kynhneigð, klám, trúmál og trúarlegar athafnir, stjórnmálaskoðanir og þjóðerni. Notendur sem fá slík skilaboð skulu tafarlaust láta yfirmann eða umsjónaraðila vita.

Tölvupóstar sem vara við tölvuvírusum og spilliforritum skulu vera heimilaðir af upplýsingatæknisviði.

Tölvupóstar geta innihaldið tölvuvírusa og aðra óværu. Ef notendur, áframsenda tölvupósta með slíkt innihald er hætta á að háskólinn teljist ábyrgur. Eins er hætta á að með því að opna slíka tölvupósta sé verið að opna leið fyrir óværu inn á kerfi háskólans og því þurfa notendur að gæta fyllstu varkárni.

Tölvupóstur nemenda við Háskólann á Bifröst, @bifrost.is, er ekki skilgreindur sem eign háskólans. Ef um ræðir öryggisatvik eða rökstuddan grun um brot á reglum háskólans, kann slíkt að fela í sér skoðun á innihaldi tölvupósts nemenda í öryggisskyni. Slíkt verði þó eingöngu skoðað ef brýna nauðsyn ber til, verði þá farið eftir verklagsreglum við skoðun á tölvupósti eða gögnum nemenda. Kom til slíkrar skoðunar skal viðkomandi nemenda

tilkynnt um hana fyrirfram, nema slíkt sé ómögulegt t.d. ef slíka skoðun fer fram vegna yfirstandandi netárásar og skal þá nemenda tilkynnt um það svo fljótt sem auðið er.

Starfsfólk og verktakar Háskólans á Bifröst skulu athuga að allt efni og öll gögn geymd, send eða viðtekin á tölvupóstfang skólans eru aðgengileg og teljast ekki einkamál. Öll gögn sem fara um póstþjóna skólans eru vistuð og geta sætt skoðun á vegum háskólans ef þörf krefur, s.s. vegna viðbragða við atvikum s.s. netárásum eða vefveiðum, vegna lengri fjarveru notanda sem krefst þess að nálgast þarf gögn í pósthólfi hans til að tryggja hagsmuni Háskólans á Bifröst. Kom til slíkrar skoðunar skal viðkomandi notanda tilkynnt um hana fyrirfram, nema slíkt sé ómögulegt t.d. ef slíka skoðun fer fram vegna yfirstandandi netárásar og skal þá notendum tilkynnt um það svo fljótt sem auðið er.

Tölvupóstar sem eru sérstaklega merktir sem einkamál eru ekki rýndir nema vegna viðbragða við atvikum s.s. netárásum eða vefveiðum, ef brýn nauðsyn þykir. Þá skal ávallt upplýsa viðkomandi um skoðunina, ef þess er kostur og bjóða honum að vera viðstaddur. Ef ekki reynist unnt að láta vita fyrirfram um skoðunina skal upplýsa notanda strax og hægt er.

Sýna skal að gæslu þegar viðtekinn tölvupóstur er áframsendur þar sem hann getur innihaldið gögn sem njóta verndar höfundaréttar.

Starfsmenn og fulltrúar nemenda geta haft aðgang að póstlistum til að ná til fjölda notenda. Þeir skulu gæta fyllstu varúðar við meðferð þessara upplýsinga og þeim er ekki heimilt að gefa öðrum aðgang að póstlistum. Einnig skulu póstlistar eingöngu vera notaðir í BCC til að tryggja að upplýsingar um tölvupóstfang einstaklinga séu ekki öllum sýnilegir. Einnig skal tryggja að slíkum dreifðum pósti sé ekki hægt að svara til allra (reply to all).

Úthlutun á tölvupóstfangi háskólans til verktaka og gesta skal vera háð leyfi frá yfirmanni eða umsjónaraðila.

13 Ruslpóstar (spam)

Tilgangur

Þessi stefna bannar alla notkun ruslpósta í tölvupóstkerfum háskólans og segir til um hvernig skal fara með slíka tölvupósta og draga úr áhættu af slíkum póstum.

Umfang

Þessi stefna gildir um alla notendur sem fá úthlutað tölvupóstfangi frá Háskólanum á Bifröst.

Stefna

Háskólinn á Bifröst líður enga notkun ruslpósts frá neinu tölvupóstfangi háskólans.

Notendur sem senda ruslpóst með nafni skólans eða frá hugbúnaði háskólans á einhvern hátt eða vísa í einhverja af vefsíðum háskólans eru að brjóta gegn stefnu háskólans.

Allir notendur skulu vera á varðbergi og umsvifalaust eyða öllum ruslpóstum sem þeir fá og ef þeir eru í vafa um eðli tölvupóstsins skulu þeir ráðfæra sig við upplýsingatæknisvið.

Upplýsingatæknisviði skal innleiða kerfi til þess að sporna við ruslpósti.

14 Þráðlaust net

Tilgangur

Stefnan tekur til aðgangs og notkunar á þráðlausum netum háskólans til að tryggja örugga starfsemi háskólans.

Umsvif

Þessi stefna tekur til allra notenda og tækja sem nýta þráðlaus net háskólans.

Stefna

Háskólinn á Bifröst veitir notendum þráðlausan netaðgang í húsakynnum háskólans. Allir notendur sem fá aðgang að þráðlausu neti háskólans, skulu nota veittan öruggan aðgang með lykilorði og gestir fá aðgang að gestaneti með lykilorði.

Notendur skulu bera ábyrgð á notkun sinni á þráðlausu neti háskólans.

Allir þráðlausir sendar í notkun í húsakynnum skólans skal stýrt af upplýsingatæknisviði. Ósamþykkt uppsetning þráðlauss búnaðar eða notkun óviðkomandi búnaðar í húsakynnum háskólans er óleyfileg.

Upplýsingatæknisvið mun gera könnun á þráðlausa netinu til að tryggja starfsemi og að engir óleyfilegir sendar séu til staðar.

Upplýsingatæknisvið getur slökkt fyrirvaralaust á öllum þráðlausum búnaði tengdum netinu sem er talin að stofni kerfum, gögnum og notendum háskólans í hættu.

Allur tölvubúnaður og tæki sem notuð eru til að tengjast þráðlausu neti háskólans skulu háðar viðurkenndum öryggiskröfum.

Notendur þráðlauss aðgangs skulu tilkynna tafarlaust til upplýsingatæknisviðs háskólans öll atvik eða grun um óleyfilega uppsetningu þráðlauss búnaðar.

15 Stjórnun breytinga á upplýsingatæknikerfum

Tilgangur

Að stýra breytingum á upplýsingatæknikerfum á fyrirsjáanlegan og kerfisbundinn hátt þannig að notendur geti skipulagt starf og nám í samræmi við fyrirhugaðar breytingar. Breytingar á upplýsingatæknikerfum krefjast skipulagningar, vandaðs eftirlits og eftirfylgni til að draga úr neikvæðum áhrifum á notendur og upplýsingatæknikerfi.

Umsvif

Þessi stefna á við um allar breytingar sem hafa áhrif á notkun upplýsingatæknikerfa háskólans. Til dæmis breytingar, uppfærslur og bætur á hugbúnaði, vélbúnaði, tölvukerfum og tengdum verklagsreglum. Stefnan á einnig við um allar breytingar sem koma að stjórnun húsnæðis, svo sem kæli og hitakerfa og aðgangskerfa, þar sem þau hafa áhrif á starfsemi upplýsingatæknikerfa.

Stefna

Sérhver breyting sem hefur áhrif á eða eru hluti af hugbúnaði, tölvukerfum, vélbúnaði, netkerfum og breytingar á stjórnun aðgangs, er háð stefnu um breytingastjórnun og skal fylgja verklagsreglum um breytingastjórnun.

Allar breytingar sem koma fram sem viðbót eða breyting á þjónustuskrá eða ef þjónusta er fjarlægð úr þjónustuskrá, skal falla undir þessa stefnu. Einnig þegar þjónusta er færð frá einum þjónustuaðila yfir á annan.

Breytingar skulu flokkaðar eftir mikilvægi í þrjá flokka, almennar breytingar, mikilvægar breytingar og neyðar breytingar.

Eigendur upplýsingatæknikerfa skulu hafa umsjón með

- Tímasetningu breytinga.
- Skilgreiningu á hver verða áhrif breytinga.
- Hvaða aðgerðum er beitt til að tryggja að starfsemi háskólans verði fyrir sem minnstri truflun.

Eigendur upplýsingatæknikerfa skulu fara yfir og meta allar beiðnir um breytingar og tryggja að upplýsingaflæði sé fullnægjandi.

Allar óskir um breytingar skulu vera lagðar fram í samræmi við reglur um verklag og ferli um breytingastjórnun þannig að tími sé til að fara yfir beiðnina, ákvarða og fara yfir hugsanleg áhrif á starfsemi háskólans og taka ákvörðun um að leyfa eða seinka beiðninni.

Eigendur upplýsingatæknikerfa geta neitað fyrirhugaðri eða ótímabærri breytingu vegna, ófullnægjandi skipulagningar, ófullnægjandi varúðarráðstafana, tímasetning hafi neikvæð

áhrif á lykilstarfsemi eða ef ekki er hægt að fá fullnægjandi yfirsýn á hvað breytingin felur í sér svo sem vegna orlofstíma, leyfa eða vegna sérstakra viðburða.

Notendur skulu frá upplýsingar um fyrirhugaða breytingu í samræmi við verklagsreglur um breytingastjórnun.

Halda verður skrá um eftirfarandi atriði fyrir allar breytingar sem og allar aðrar upplýsingar sem varða málið

- Ákvörðun og tími byggt á mati.
- Áætluð tímalengd framkvæmdar breytinga.
- Samskiptaupplýsingar.
- Tegund og eðli breytingarinnar.
- Vísbending um árangur.
- Skrá alla hnökra á framkvæmd og niðurstöðu breytinga.

Eftir að breyting hefur verið framkvæmd skal fara yfir niðurstöður og athugað hver voru áhrif á umhverfi, var tilgangi náð, var breyting til bóta, eða tókst breyting eins og til var ætlast. Einnig skal skoða hvort verklagsreglum var fylgt eða er ástæða til að breytinga á verklagsreglum.

16 Reglur um öryggi upplýsingatæknikerfa

Tilgangur

Markmið þessarar stefnu er að stuðla að öruggri stjórn og aðgangi að upplýsingatæknikerfum háskólans.

Umsvif

Þessi stefna gildir um öll upplýsingatæknikerfi háskólans.

Stefna

Upplýsingatæknikerfi skulu nota hugbúnað sem er studdur af þróunaraðila, söluaðila eða framleiðanda, með ábyrgð um lagfæringu vegna galla og/eða öryggisvandamála.

Viðhalda skal upplýsingatæknikerfum með reglulegum uppfærslum og viðgerðum til að bregðast við öryggisveikleikum og rekstrarlega mikilvægum göllum.

Upplýsingatæknikerfi skulu vera varin gegn skaðlegum hugbúnaði.

Upplýsingatæknikerfi skulu vera sett upp til að koma í veg fyrir óleyfilega notkun og vernda geymslu, sendingu og vinnslu gagna háskólans.

Fylgjast skal með öllum upplýsingatæknikerfum með tilliti til óleyfilegrar notkunar og grípa til aðgerða í samræmi við stefnu um öryggistengd atvik.

Eigendur upplýsingatæknikerfa eru ábyrgir fyrir reglulegri uppfærslu, innleiðingu öruggra stillinga og eftirliti með óleyfilegri notkun.

17 Endurskoðun og eftirlit

Tilgangur

Þessi stefna setur reglur um endurskoðun á upplýsingatæknikerfum háskólans.

Umfang

Stefnan nær yfir notendur og upplýsingatæknikerfi háskólans. Einnig tekur stefnan til allra notenda sem tengjast upplýsingatæknikerfum háskólans í gegnum eigin tölvur og snjalltæki.

Stefna

Upplýsingatæknisvið skal framkvæma endurskoðun á upplýsingatæknikerfum háskólans. Endurskoðun getur einnig verið samþykkt og framkvæmd af sérfræðingum utan háskólans samkvæmt beiðni.

Endurskoðun getur meðal annars falið í sér:

- Aðgangur að gögnum úr vinnslukerfum sem tengjast starfsemi háskólans.
- Notkun aðgangstýringar að svæðum og vélbúnaði.
- Framkvæmd stefnu um prófun á tölvuárásum.
- Endurskoðun lykilorða

Tilkynna skal öllum aðilum sem eru hluti af endurskoðun að endurskoðun sé í framkvæmd.

Við lok endurskoðunar skal skrá niðurstöður og gera viðeigandi úrbætur á verklagsreglum og kerfum sem skal notað til hliðsjónar við næstu endurskoðun.

18 Netbeinar og netdeilar

Tilgangur

Þessi stefna skilgreinir öryggisstillingar fyrir netbeina og netdeila sem tengjast neti háskólans.

Umsvif

Allir netbeinar og netdeilar sem tengjast netum háskólans falla undir þessa stefnu.

Stefna

Engir beinn notendaaðgangur skal vera settur á netbeina og netdeila. Notendaaðgangur fyrir netbeina og netdeila er í gegnum öruggt net með viðurkenndum og skráðum tengingarleiðum.

Lykilorð á netbeini verða að vera á öruggu dulkóðuðu formi. Netbeinir verður að hafa lykilorð stillt á það lykilorð sem er í gildi og upplýsingatæknisvið stýrir.

Eftirfarandi er bannað:

- IP stýrðar dreifingar
- Pakkar viðteknir á netbeini sem eru með ógild vistföng (t.d. RFC1918 vistföng)
- TCP lítil þjónusta
- UDP lítil þjónusta
- Öll „source routing“
- Öll vefþjónusta keyrð á netbeini

Nota skal staðlaða SNMP (Simple Network Messaging Protocol) fyrir stjórnun og vöktun á vélbúnaði.

Netbeinar og netdeilar skulu vera hluti af öryggisstjórnunarkerfi háskólans undir eftirliti kerfisstjóra.

Allir netbeinar og netdeilar skulu vera skýrt merktir með skilaboðum um takmarkaðan aðgang.

Notendur verða að hafa leyfi frá upplýsingatæknisviði til að fá aðgang að eða stilla netbeina og netdeila.

Allur aðgangur og skipanir framkvæmdar á netbeinum og netdeilum skulu vera skráðar.

19 Uppsetning hugbúnaðar

Tilgangur

Stefnan tryggir að allur hugbúnaður á tölvum háskólans er settur upp á öruggan og skilvirkan máta. Einnig tekur stefnan til þess að eingöngu er notaður leyfilegur hugbúnaður, sannanlega fengin með löglegum hætti.

Umsvif

Þessi stefna nær yfir alla notendur og búnað hvort sem er í eigu háskólans eða einkaeign með aðgang að gögnum háskólans. Búnaður er meðal annars tölvur, netþjónar og snjalltæki.

Stefna

Öll uppsetning tölva háskólans skal vera framkvæmd af upplýsingatæknisviði fyrir afhendingu til notenda og tenging við sjálfvirkar uppfærslur á stýrikerfi skal vera tryggður.

Upplýsingatæknisvið skal setja upp allan nauðsynlega hugbúnað á tölvum sem er úthlutað til starfsmanna. Auk þess skal vera uppsett vírusvörn og vörn gegn spilliforritum til að tryggja öryggi gagna.

Setja skal upp nýjustu útgáfu hugbúnaðar samkvæmt aðkeyptum leyfum.

Ekki skal setja upp ólöglegan eða óleyfilegan hugbúnað.

Starfsmönnum er óheimilt að setja upp hugbúnað á tölvur háskólans að eigin frumkvæði og beiðnir um hugbúnað skulu sendar til upplýsingatæknisviðs.

Í undantekninga tilvikum getur notandi fengið að tengja eigin tölvu við net háskólans. Ef notandi hefur leyfi til að nota eigin tölvu þá skal hann tryggja að á tölvunni sé enginn óleyfilegur eða ólöglegur hugbúnaður. Tölvan skal einnig hafa alla nauðsynlega vörn gegn vírusum og spilliforritum

Uppsetning hugbúnaðar á snjallsíma og snjalltæki er framkvæmd af notendum sem skulu trygga að á þeim tækjum séu engin óleyfilegur eða ólöglegur hugbúnaður.

20 Prófun með tölvuárásum

Tilgangur

Þessi stefna setur reglur um prófanir á tölvuárárásum sem líkir eftir netárásum og framkvæmd þeirra, með það að markmiði að bæta varnir fyrir upplýsingatæknikerfi háskólans. Þessi stefna skilgreinir hlutverk og ábyrgð stjórnenda háskólans, upplýsingatæknisviðs og ytri endurskoðenda.

Umsvif

Almennt gildissvið þessarar stefnu á við um alla notendur og upplýsingatæknikerfi háskólans

Stefna

Við prófanir á tölvuárásum skal tryggja að prófanir beinist að viðeigandi upplýsingatæknikerfum háskólans og með það markmið að sannreyna öryggi og réttleika upplýsingatæknikerfa og gagna.

Allar prófanir á tölvuárásum sem fram fer á upplýsingatæknikerfum verður að vera í samræmi við viðeigandi lög og reglur og sýna skal sérstaka aðgát ef að prófanir beinast að upplýsingatæknikerfum sem innihalda viðkvæm gögn.

Tölvuárás á innra net er til að bera kennsl á hvers kyns veikleika og öryggisgalla á upplýsingatæknikerfum háskólans sem felur í sér en takmarkast ekki við netþjóna, eldveggi, netdeila, netbeina, prentara, vinnustöðvar, öryggistæki, jaðartæki og hvers kyns hugbúnað. Að auki geta prófanir falið í sér prófunaraðgerðir með og án innskráningar.

Tölvuárásir á vefforrit eru til að greiningar á hvers kyns veikleikum, öryggisgöllum eða ógnum við hugbúnað í eigu háskólans. Tölvuárásir geta falið í sér þekktar skaðlegar árásir á hugbúnað, þar á meðal handvirkar og sjálfvirkar tölvuárásir.

Samfélagsmiðlatengdar tölvuárásir eru gerðar til að prófa þekkingu og varkárni notenda gegn árásum tengdum samfélagsmiðlum og veita aukna þekkingu á atriðum þar sem veikleikar koma í ljós.

Það skal tekið fram að stefnan veitir ekki tæmandi upplýsingar um prófanir sem eru gerðar með tölvuárásum.

21 Vélbúnaður og hugbúnaður

Tilgangur

Stefna um vél- og hugbúnað styður við fyrirbyggjandi og viðvarandi viðhald og stjórn á tölvu- og hugbúnaði í eigu Háskólans á Bifröst.

Umsvif

Þessi stefna nær yfir alla notkun á tölvu- og hugbúnaði í eigu Háskólans á Bifröst

Stefna

Allur tölvubúnaður skal geta keyrt nauðsynlegan hugbúnað á hagkvæman og skilvirkan hátt.

Reglubundið skal meta hvort þörf er á að endurnýja tölvubúnað til að fylgja þróun og öryggi í upplýsingatækni.

Upplýsingatæknisvið skal í samvinnu við fjármálasvið vinna að hagkvæmum innkaupum með skilgreindri þörf og ítarlega tilgreindri ábyrgð.

Upplýsingatæknisvið fylgist með að gallaðir hlutir í ábyrgð verði viðgerðir tímanlega og að viðgerður og/eða umframbúnaður sem fellur ekki undir núverandi ábyrgð skal uppfylla allar öryggis og verklagsreglur háskólans

Upplýsingatæknisvið skal setja upp allan net- og tölvubúnað og tryggir að búnaður sé samhæfður núverandi kerfum og hugbúnaði.

Upplýsingatæknisvið skal tryggja að allur tölvubúnaður hafi nauðsynlegan hugbúnað til að starfa sem skildi og uppfylli þarfir notenda fyrir starfsemi háskólans.

22 Stefna um hlutlaust svæði

Tilgangur

Þessi stefna setur reglur um tæki og búnað sem staðsettur er utan eldveggs háskólans.

Umsvif

Tæki og búnaður sem snúa að netinu og sem eru hluti af starfsemi háskólans teljast hluti af "hlutlausu svæði" (DMZ). Þessi stefna tekur einnig til hvers kyns starfsemi sem er vistuð eða hýst hjá þjónustuaðila.

Stefna

Tæki og búnaður sem snúa að netinu og eru utan eldveggs háskólans eru sérstaklega viðkvæm fyrir árásum.

Tæki og búnaður sem fellur undir gildissvið þessarar stefnu verður að setja upp í samræmi við staðla sem vísað er til, nema undanþága sé fengin frá upplýsingatæknisviði.

Búnaður og tæki innan gildissviðs þessarar stefnu verður að vera undir stjórn aðila sem eru samþykktir af upplýsingatæknisviði fyrir DMZ kerfi.

Samningar við þjónustuaðila sem hýsa tæki og búnað háskólans skulu tilgreina ábyrgð og öryggi búnaðar með skilgreindu þjónustustigi.

Samningar skulu tryggja að starfsemi þjónustuaðila samræmist þessari stefnu.

Þjónustuaðilar bera ábyrgð á eftirfarandi:

- Búnaður verður að vera skráður með eftirfarandi upplýsingar:
    - Tengiliðir og staðsetning.
    - Vélbúnaður og stýrikerfi/útgáfa.
    - Lykilorðshópa fyrir aðgang.
- Netviðmót verður að hafa viðeigandi lénsnafnaþjónsskrár (að lágmarki A og PTR færslur).
- Lykilorðshópum verður að viðhalda í samræmi við stefnu háskólans um lykilorð.
- Veita skal upplýsingatæknisviði aðgang að búnaði og kerfisskrám sé þess óskað.
- Breytingar á núverandi búnaði og uppsetning nýs búnaðar verða að fylgja verklagsreglum og stefnu um breytingastjórnun.

Til að tryggja samræmi við þessa stefnu skal upplýsingatæknisvið endurskoða DMZ búnað reglulega.

Allan búnað skal setja upp í samræmi við eftirfarandi:

- Vélbúnaður og stýrikerfi verða að vera samþykkt af upplýsingatæknisviði og í samræmi við stefnu um uppsetningu vélbúnaðar.
- Allar bætur og uppfærslur sem seljandi búnaðar og upplýsingatæknisvið mæla með verða að vera virkjaðar tímanlega. Þetta á einnig við um þjónustu sem er óvirk tímabundið eða varanlega.
- Þjónusta og hugbúnaður sem þjóna ekki lengur hlutverki skulu gerð óvirk.
- Traust sambönd milli kerfa skulu vera skjalfest og þau verða að vera samþykkt af upplýsingatæknisviði.
- Þjónusta og hugbúnaður skal vera varinn með aðgangsstýringum.
- Ávallt skal beita traustri og öruggri þjónustu eða samskiptareglum.
- Fjarstjórnun verður að fara fram á öruggum tengingum (t.d. dulkóðaðar nettengingar með SSH eða IPSEC) eða stjórnborðsaðgangi óháð DMZ netum. Þar sem aðferðafræði fyrir öruggar tengingar er ekki tiltæk, verður að nota einstakt lykilorð (DES/SofToken) fyrir öll aðgangsstig.
- Allar uppfærslur á búnaði skal framkvæma í gegnum traustar tengingar.
- Öryggistengda atburði skal ávallt skrásetja. Öryggistengdir atburðir innihalda en takmarkast ekki við eftirfarandi:
    - Bilun í innskráningu notanda.
    - Misbrestur á að fá aðgang að takmörkuðum svæðum.
    - Brot á reglum um aðgang.
- Upplýsingatæknisvið skal taka ákvörðun um allar beiðnir um undanþágu.

23 Hugbúnaðaruppfærslur og bætur fyrir upplýsingatæknikerfi

Tilgangur

Tilgangur þessarar stefnu er að tryggja öryggi upplýsingatækniauðlinda háskólans sem veitt er með hugbúnaðaruppfærslum og bótum.

Umsvif

Stefnan tekur til upplýsingatæknikerfa háskólans og notenda sem hafa aðgang að þeim.

Stefna

Eigendur upplýsingatæknikerfa bera ábyrgð á innleiðingu á hugbúnaðaruppfærslum og bótum sem er undir þeirra stjórn.

Skilgreina skal áætlun og ferli varðandi stýringu á hugbúnaðaruppfærslum og bótum eða stillingarbreytingum.

Bregðast skal við veikleikum eins fljótt og auðið er. Ef lausn eða úrbætur eru ekki tiltækar verður að meta og samþykkja mótvægisaðgerðir.

Forgangsraða skal uppsetningu á uppfærslum og bótum með tilliti til alvarleika veikleika.

Upplýsingatæknisvið hefur umsjón með og stjórnar uppfærslum fyrir stýrikerfi á tölvum og netþjónum háskólans. Leitast skal við að uppfærslur fyrir stýrikerfi séu sjálfvirkar og ber að skrá og meta þörf og hugsanlegar afleiðingar allra uppfærsla og bera saman niðurstöðu við upprunalegt mat.

Mikilvægi viðgerða/uppfærslna

Stig	Lýsing
Nauðsynleg	Veikleiki sem gæti leyft sjálfvirka keyrslu kóða án stjórnar notenda. Þessar aðstæður fela í sér sjálfsútbreiðslu spilliforrita (t.d. netorma), eða þar sem keyrsla kóða á sér stað án viðvarana eða skipunar. Þetta gæti þýtt að vafra um vefsíðu eða opna tölvupóst.
Mikilvæg	Veikleiki þar sem notkun gæti leitt til skerðingu á öryggi, nákvæmni eða aðgengi gagna. Tölva eða tæki hefur fengið öryggisviðvaranir eða notenda aðgerðir fara ekki eftir aðvörunum.
Meðal	Veikleikinn er óverulegur þar sem aðgangur er stýrður með auðkenningu eða öðrum undantekningum.
Væg	Veikleikinn er óverulegur og matsatriði er hvort nota eigi öryggisuppfærslu á viðkomandi kerfi.

24 Áhættustýring

Tilgangur

Að skilgreina áhættustýringu sem miðar að því að tryggja réttileika, aðgengi, tiltækileika og rekjanleika gagna og auka öryggi upplýsingatæknikerfa háskólans.

Umsvif

Þessi stefna gildir um öll upplýsingatæknikerfi og notendur sem að hafa aðgang að þeim.

Stefna

Öll upplýsingatæknikerfi háskólans þurfa að tryggja eins og kostur er réttleika, tiltækileika og leynd gagna.

Áhættumat á upplýsingatæknikerfum háskólans skal framkvæma reglulega þar sem ásættanleg áhætta er skilgreind.

Áhættumat skal framkvæmt á öllum upplýsingatæknikerfum í notkun og skal þar að auki vera lokið fyrir kaup á nýjum upplýsingatæknikerfum eða ef verulegar breytingar verða á núverandi kerfum.

Innleiða skal verklagsreglur fyrir framkvæmd áhættumats og skilgreina skal hvernig taka skal á áhættu sem er meiri en ásættanleg áhætta.

Áhættumat skal framkvæmt einu sinni á ári ef um er að ræða upplýsingatæknikerfi sem hýsa mjög viðkvæm gögn en annars á tveggja ári fresti.

Áhætta skal metin út frá líkum á ógn og hversu alvarlegar afleiðingar það hefur fyrir starfsemi háskólans.

Áhættu sem greinist með áhættumati verður að stjórna til að takmarka hugsanlegan skaða eða samþykkja áhættuna áður en upplýsingatæknikerfið er tekið í notkun.

Áhætta sem ekki er varist með nokkrum hætti má aðeins samþykkja fyrir hönd háskólans af einstaklingi með viðeigandi valdsvið.

Áhættumat skal tilgreina mögulegar mótvægisaðgerðir til að minnka áhættu og meta hversu mikil áhrif þær hafa.

Eigendur upplýsingatæknikerfa bera ábyrgð á framkvæmd áhættumats og innleiðingu mótvægisaðgerða fyrir upplýsingatæknikerfi undir þeirra stjórn.

25 Öryggi netþjóna

Tilgangur

Tilgangur þessarar stefnu er að skilgreina leiðbeiningar og verklagsreglur fyrir uppsetningu, stjórnun og rekstur netþjóna í eigu eða rekstri háskólans. Virk innleiðing þessarar stefnu mun lágmarka óviðkomandi aðgang að upplýsingum og upplýsingatæknikerfum Háskólans á Bifröst.

Umsvif

Þessi stefna gildir um netþjónabúnað sem er í eigu eða er rekinn af háskólanum og allra notenda sem hafa aðgang að netþjónum. Þessi stefna er sérstaklega fyrir búnað á innra neti háskólans. Fyrir örugga uppsetningu búnaðar utan innra nets háskólans er þörf á hlutlausu svæði samanber stefnu um hlutlaust svæði.

Stefna

Upplýsingatæknisvið skal skilgreina leiðbeiningar og verklagsreglur fyrir uppsetningu netþjóna.

Leiðbeiningar og verklagsreglur um uppsetningu netþjóna skulu vera virkar og endurskoðaðar reglulega.

Kerfistjóri skal tryggja að uppsetningar á netþjónum séu í samræmi við leiðbeiningar og verklagsreglur.

Kerfisstjóri skal innleiða öryggisstýringar og meta öryggi netþjóna.

Skrá skal kerfisupplýsingar áður en nýr netþjónn er tekinn í notkun.

Skrá skal allar meiri háttar breytingar á tilgangi netþjóns, uppsetningu og staðsetningu.

Einungis skal setja upp stýrikerfi sem eru uppfærð og studd af framleiðanda og uppsetning stýrikerfis skal vera í samræmi við útgefna staðla.

Nýjustu öryggisbætur skulu vera settar upp á netþjónum eins fljótt og hægt er, eina undantekningin er þegar slíkt myndi trufla starfsemi háskólans.

Kerfisstjóri skal fylgjast með netþjónaskrám og sjá til þess að hægt sé að endurheimta þjónustu netþjóns.

Alltaf skal nota reglu um minnsta nauðsynlegan aðgang til að framkvæma hverja aðgerð.

Nota skal aðgang með lágmarks forréttindi þegar mögulegt er.

Notendaaðgangur að netþjónum skal vera með sterkt lykilorð sem er breytt reglulega.

Fjölþáttaauðkenning skal vera notuð fyrir aðgang að netþjónum.

Nota skal trausta tengingu *(t.d. VPN, dulkóðaðar nettengingar með SSH eða IPSec.*) við uppsetningu og uppfærslu fyrir utan net háskólans

Ef traust tenging er tiltæk *(t.d. tæknilega framkvæmanleg), v*erður forréttinda aðgangur að fara fram á traustri tengingu (*t.d. dulkóðaðar nettengingar með SSH eða IPSec).*

Netþjónar skulu vera staðsettir í húsnæði með umhverfisstýringum til þess að vernda netþjóna gegn tjóni eins og frá vatnsleka eða vegna hitabreytinga.

Netþjónar skulu ekki notaðir í hússnæði eða á svæðum sem eru ekki tryggð með aðgangsstjórnun.

Þjónusta og hugbúnaður sem ekki eru lengur í notkun skulu vera gerð óvirk þar sem það er hægt.

Aðgangsskrár frá netþjónakerfum skulu skoðaðar reglulega af starfsmönnum upplýsingatæknisviðs.

Starfsmenn skulu fá þjálfun í rekstri netþjóna.

Eftirliti skal stýrt af starfsmönnum upplýsingatæknisviðs og úrbætur skulu innleiddar í samræmi við niðurstöðu endurskoðunar.