Efnisyfirlit

Upplýsingaöryggisstefna NTÍ

1. Markmið og tilgangur upplýsingaöryggisstefnunnar

Það er stefna stjórnar að lágmarka rekstraráhættu og stuðla að eftirfylgni stofnunarinnar við lög og reglur er lúta að rekstri upplýsingakerfa. Lágmörkun áhættu við rekstur upplýsingakerfa er m.a. fólgin í því að gera ráðstafanir sem miða að því að stýra rekstraráhættu, koma í veg fyrir hagsmunaárekstra og tryggja gagnsæi hjá stofnuninni. Einnig ber að tryggja öryggi upplýsinga, þ.e. að tryggja að aðeins þeir sem hafa til þess heimild, hafi viðeigandi aðgang þegar þeir þurfa hann og að upplýsingarnar séu réttar og óspilltar.[1]

Í þeim tilgangi að lágmarka rekstraráhættu sem kann að skapast af ófullnægjandi upplýsingakerfum skal umsjón upplýsingakerfa úthýst til fyrirtækis sem hefur gott orðspor og þekkingu á því sviði. Þjónustuaðili í upplýsingatækni sem samið er við um heildarrekstur upplýsingatæknikerfa skal að lágmarki uppfylla ISO27001 upplýsingastjórnunarstaðalinn.[2] Með upplýsingakerfum er átt við þau vélrænu kerfi sem koma að vinnslu upplýsinga ásamt öllum tengingum að, frá og á milli þeirra.[3]

Stefnunni skulu fylgja gæðamarkmið á einstökum sviðum upplýsingatækni og frávikaskráning skal fara fram með skipulögðum hætti.[4] Öryggisstjórnun og stjórnunarferli beinast að hagsmunum stofnunarinnar. Þess vegna beinist stefnan einnig að:

- Leynd - Til að tryggja að upplýsingar séu eingöngu aðgengilegar þeim sem til þess hafa heimild.
- Réttleiki - Til að standa vörð um nákvæmni og heilleika upplýsinga og úrvinnsluaðferða.
- Tiltækileiki - Til að tryggja að þeir sem til þess hafa heimild, hafi aðgang að upplýsingum og tengdum eignum stofnunarinnar eftir þörfum.

2. Skipulag

2.1 Ábyrgð

Í ljósi smæðar í yfirbyggingu hjá NTÍ er rekstri, viðhaldi, hýsingu og afritun allra upplýsingakerfa auk hönnunar og þróunar, úthýst til þjónustuaðila innanlandsStjórn NTÍ ber sábyrgð á rekstri og áhættustýringu upplýsingakerfa sinna[5]. Það er í samræmi við afstöðu FME um að eftirlitsskyldur aðili beri stjórnunarlega ábyrgð á að rekstur upplýsingakerfa uppfylli þær kröfur sem til hans eru gerðar[6]. Þetta á við hvort sem rekstri upplýsingakerfa er útvistað að hluta til eða í heild sinni. Stjórn NTÍ ber ábyrgð á að staðfesta upplýsingaöryggisstefnuna sem og þær viðmiðunarreglur sem hún inniheldur. Framkvæmdastjóri ber ábyrgð á að framfylgja stefnu í stjórnun upplýsingaöryggis og allir starfsmenn og þjónustuaðilar NTÍ bera ábyrgð á að fylgja stefnunni. Upplýsingaöryggisstefnan skal vera viðauki við þjónustusamning NTÍ og þjónustuaðila um rekstrarþjónustu upplýsingakerfa.

2.2 Stjórnun[7]

Gæðanefnd NTÍ[8] hefur eftirfarandi hlutverk á sviði upplýsingaöryggismála undir stjórn framkvæmdastjóra:

- Vera samráðsvettvangur öryggismála fyrirtækisins.
- Gera tillögur um öryggismarkmið, áætlanir og stefnur.

[1] Sbr. inngang í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[2] Sbr. gr. 2.2.7 í áhættustýringarstefnu Viðlagatryggingar Íslands
[3] Sbr. grein 1.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[4] Sbr. grein 4.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[5] Sbr. grein 3.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[6] Sbr. grein 11.8 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[7] Sbr. grein 4.2.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[8] Gæðanefnd samanstendur af öllum starfsmönnum NTÍ.

- Samræma mótun stefnu og viðmiðunarreglna.
- Skilgreina reglur um aðgangsstjórnun og ákveða reglur um notkun upplýsinga
- Setja eftirlitsmarkmið og velja eftirlitsaðgerðir.
- Hafa eftirlit með fylgni við upplýsingaöryggisstefnu og verklagsreglur stofnunarinnar.
- Skipuleggja sérstök öryggisverkefni.
  Framkvæmdastjóri hefur lokavald í öllum ákvörðunum gæðanefndar.

Gæðafulltrúi annast málefni er varða upplýsingaöryggi stofnunarinnar í umboði gæðanefndar.

Helstu verkefni hans eru að:

- Hafa eftirlit með og stuðla að framkvæmd upplýsingaöryggisstefnu.
- Koma af stað, samræma og vakta verkefni er varða upplýsingaöryggi.
- Hafa umsjón með að farið sé eftir stefnunni og öryggisreglum.
- Viðhalda innri og ytri samböndum í tengslum við öryggismál.
- Halda utan um aðgangsstýringar að upplýsingakerfum stofnunarinnar annarra en starfsmanna þjónustuaðila viðkomandi kerfis.

Eigandi gagna er NTÍ.
Umsjónarmaður er sá starfsmaður NTÍ sem er tengiliður við þjónustuaðila vegna notkunar viðkomandi kerfis og ber ábyrgð á kröfum sem gerðar eru til stofnunarinnar af hálfu FME og uppfyllingu krafna vegna þjónustusamnings[9].

Ábyrgðarmaður þjónustuaðila er skilgreindur sérstaklega fyrir hvert kerfi eða búnað (þ.m.t. gögn). Hann sér um aðgangsveitingu að gögnum eða kerfum að beiðni eiganda. Hann fer með daglega stjórnun og öryggi þeirra kerfa sem hann ber ábyrgð á. Ábyrgðarmaður þjónustuaðila getur verið starfsmaður utan stofnunarinnar.
Aðrir eru þeir sem þurfa að fá aðgang að gögnum stofnunarinnar og eru ekki starfsmenn.

3. Öryggi

3.1 Öryggi tækjabúnaðar og gagna[10]

Gera skal ráðstafanir til þess að verja búnað, lagnir, kerfi og upplýsingar sem eru mikilvæg NTÍ gegn skemmdum t.d. af völdum áfalla, misnotkunar, óheimilum aðgangi, óheimilla breytinga, skemmdarverka, þjófnaðar, eldsvoða, reyks, vatns og rafmagnstruflana[11]. Öllum tækjabúnaði skal viðhaldið samkvæmt leiðbeiningum framleiðanda og þjónustuaðila hans. Tryggja skal leynd og réttleika gagna þegar tækjabúnaður er sendur til viðgerða fyrir utan umráðasvæði NTÍ eða þjónustuaðila.[12] Aðgangur að helstu rafmagns- og fjarskiptalögnum skal varinn sérstaklega.

3.1.1 Tækjabúnaður utan starfssvæðis, þ.m.t. snjalltæki

Notkun á tækjabúnaði utan starfssvæðis er háð samþykki framkvæmdastjóra. Öryggi þess búnaðar skal ekki vera minni en sambærilegs búnaðar innan starfssvæðis að viðbættri áhættu sem hlýst af notkun búnaðarins utan

[9] Sbr. grein 11.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[10] Sbr. grein 4.2.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[11] Sbr. grein 5.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[12] Sbr. skilgreiningar í markmiðum og tilgangi upplýsingaöryggisstefnunnar

svæðis. Sama gildir um búnað sem starfsmenn hafa til notkunar heima vegna vinnu sinnar. Heimilt er að hafa tölvupóst NTÍ uppsettan í snjallsímum starfsmanna, sé hann stilltur þannig að póstur geymist ekki lengur en í 6 mánuði á símanum og lágmarkskrafa til aðgangsstýringar á símanum sé 6 tölustafa lykilorð eða notkun fingrafars eða augnskanna. Notkun mynsturs til aðgangsstýringar er ekki heimil.

3.1.2 Förgun og endurnýting tækjabúnaðar

Áður en tækjabúnaður er endurnýttur eða honum fargað skal tryggja að öllum gögnum á honum hafi verið eytt þannig að þau verði ekki aðgengileg óviðkomandi, þetta á einnig við um færanlega gagnamiðla. Ef harðir diskar, geisladiskar og disklingar skemmast skal sjá til þess að þeir verði algjörlega eyðilagðir áður en þeim er hent.

3.2 Öryggi fasteignar

Þjónustuaðili öryggiskerfis NTÍ skal skrá hvenær öryggiskerfi fasteignar er sett á og hvenær það er tekið af. Framkvæmdastjóri hefur stjórnunar- og yfirlitsaðgang að kerfinu og skal yfirfara upplýsingar eigi sjaldnar en árlega, með tilliti til eftirfarandi atriða:

- Er öryggiskerfi að jafnaði sett á að loknum vinnudegi
- Er aðgangur óviðkomandi stofnuninni nýttur (s.s. aðgangur öryggisvarða)
- Eru sameiginlegir aðgangar nýttir
- Er aðgangi starfsmanns sem hefur lokið störfum lokað
- Hefur öryggiskerfi farið í gang á tímabilinu og ef svo, hver voru viðbrögð þjónustuaðila
- Lá öryggiskerfið niðri á einhverjum tímapunkti á tímabilinu og ef svo, var NTÍ látin vita.
- Skýrsla um úttektina skal vistuð á lista yfir innri úttektir á innraneti.

4. Flokkun, áhættumat og viðbragðsáætlun eigna

4.1 Listi yfir eignir

Halda skal uppfærðan lista yfir einstök upplýsingakerfi sem eru mikilvæg starfsemi og rekstraröryggi stofnunarinnar, ásamt upplýsingum um staðsetningu eignanna og lýsingu á þeim.[13]
Hverri þessara eigna skal úthlutað umsjónarmanni úr röðum starfsmanna NTÍ auk ábyrgðarmanns hjá þjónustuaðila sem ber ábyrgð á öryggi viðkomandi eignar skv. samningi við NTÍ.

Eignir stofnunarinnar skulu metnar út frá eftirfarandi flokkum og skilgreiningum:

4.1.1 LEYND

HÁTT	Mjög viðkvæmar. Upplýsingar sem munu valda miklu tjóni ef þær eru birtar án leyfis eða notaðar í óheiðarlegum tilgangi.
MIÐLUNGS	Viðkvæmar. Upplýsingar sem gætu valdið tjóni ef þær yrðu misnotaðar og birtust utan VTÍ án leyfis.
LÁGT	Almennar upplýsingar. Upplýsingar sem geta ekki skaðað ímynd VTÍ og mega birtast utan stofnunarinnar. Upplýsingar sem ekki ríkir sérstök leynd um.

Ýmsar upplýsingar falla utan þessarar flokkunar, s.s. auglýsingar, ársreikningar og kynningar sem teljast opinberar og öllum er heimill aðgangur að.

[13] Sbr. grein 4.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

4.1.2 RÉTTLEIKI

HÁTT	Ómissandi. Upplýsingar sem munu valda miklu tjóni ef réttleiki þeirra spillist.
MIÐLUNGS	Mikilvægar. Upplýsingar sem munu valda tjóni ef réttleiki þeirra spillist.
LÁGT	Eðlilegar. Upplýsingar sem munu valda óverulegu eða engu tjóni ef réttleiki þeirra spillist.

4.1.3 TILTÆKILEIKI

HÁTT	Ströng tímatakmörk. Óviðunandi ef viðkomandi upplýsingar (kerfi) eru ekki aðgengilegar. Tímatakmörk fyrir endurheimt eru innan við 72 klst. ef um stórslys er að ræða, og innan við 24 klst. fyrir minni óhöpp.
MIÐLUNGS	Tímatakmörk. Tímatakmörk fyrir endurheimt upplýsinga (kerfis) eru innan við 120 klst. ef um stórslys er að ræða, og innan við 48 klst. fyrir minni óhöpp.
LÁGT	Engin sérstök tímatakmörk. Allar upplýsingar (kerfi) með önnur endurheimtartímatakmörk.

4.2 Áhættumat upplýsingaöryggis

NTÍ skal gera kerfisbundna úttekt á áhættu er fylgir notkun eigna sinna m.t.t. starfssviðs og flækjustigs. Meta skal bæði þær hættur er fylgja núverandi upplýsingatækni sem og hættum er fylgt gætu áformuðum breytingum á þeirri tækni sem notuð er. Áhættumat er ferli sem er stöðugt í gangi og metur hættur er varða rekstur tengdan notkun upplýsingatækni. Ráðstafanir eru skilgreindar í framhaldi af matinu, ábyrgðarmaður tilgreindur ásamt því að hafa skal eftirlit með þeim. NTÍ skal ákveða viðmið fyrir ásættanlega áhættu tengda notkun upplýsingatækni m.t.t. starfssviðs og flækjustigs stofnunarinnar. Í því sambandi þarf jafnframt að endurskoða viðmiðin með reglubundnum hætti og greina áhættu af rekstri upplýsingakerfa.[14] Framkvæmdastjóri ber ábyrgð á að áhættumat skuli framkvæmt a.m.k. einu sinni á ári og auk þess sé gert áhættumat í tengslum við breytingar sem skipta máli fyrir upplýsingaöryggi, til þess að tryggja að áhættan sé innan viðmiða sem sett hafa verið fram.[15] Framkvæmd og niðurstaða áhættumatsins skal skjalfest og samþykkt ásamt tillögum til úrbóta þar sem þörf er á eftirfylgni.[16] Taka skal ákvörðun um hvort þörf sé fyrir frekari öryggisráðstafanir en tilgreindar eru í upplýsingaöryggisviðmiðum samhliða áhættumatinu.

Viðbragðsáætlun[17]

NTÍ skal útbúa viðbragðsáætlun vegna rekstrarstöðvunar upplýsingakerfa þar sem unnið skal gegn röskun á rekstri og að því að vernda mikilvæg rekstrarferli fyrir áhrifum af meiri háttar bilunum eða stóráföllum. Tryggja skal eins og unnt er órofna gagnavinnslu í neyðartilfellum eða stórslysum. Í viðbragðsáætluninni skulu skilgreind hlutverk, ábyrgð, verkefni og áhættur[18].

Áhættumat (sem lýst er í kafla 4.2) skal gefa vísbendingu um það hvaða upplýsingakerfi eru mikilvæg starfsemi NTÍ.[19] Viðbragðsáætlun upplýsingatæknikerfa (VLR238) skal gerð til að tryggja samfelldan rekstur þeirra kerfa sem teljast mikilvæg samkvæmt áhættumati auk þeirra sem falla undir tiltækileikaflokkinn „HÁTT“. Viðbragðsáætlunin skal taka til greiningar og mats á þeim einstöku þáttum sem geta brugðist og til hvaða viðeigandi ráðstafana skal grípa.

[14] Sbr. grein 2.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[15] Sbr. grein 2.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[16] Sbr. grein 2.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[17] Sbr. grein 10 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[18] Sbr. grein 10.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[19] Sbr. grein 10.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

Viðbragðsáætlunin skal innihalda eftirfarandi:
Yfirsýn yfir upplýsingakerfin sem tilheyra áætluninni[20].
Lýsingu á áfallalausnum[21].
Skýr viðmið um hvenær skuli gripið til áfallalausna[22].
Ásættanleg tímamörk rekstrarstöðvunar áður en gripið er til áfallalausna[23].
Skýr viðmið um hvenær ræsa skal neyðarhóp (framkvæmdastjóri, og/eða gæðafulltrúi ásamt fulltrúa þjónustuaðila).
Verkferlum til að koma rekstri upplýsingakerfa aftur í gang[24].
Yfirsýn yfir ábyrgðarsvið og gangsetningarferla áfallalausna[25].
Upplýsingagjöf til stjórnar, starfsmanna, viðskiptamanna og annarra aðila sem vitneskju þurfa að hafa um rekstrarstöðvun[26].
Ef endurheimtaraðgerðir hafa í för með sér notkun afrita skulu eftirfarandi atriði skilgreind[27]:
Verkferlar fyrir afritatöku til þess að tryggja áframhald þjónustu.
Prófun afritunarferla.

Viðbragðsáætluninni skal framfylgt með kennslu, æfingum og prófunum á varalausnum sem tryggja að þær virki eins og til er ætlast, eftir því sem við á. Jafnframt er mikilvægt að prófanir séu skjalfestar þannig að hægt sé að leggja mat á framkvæmd og árangur.[28]

Viðbragðsáætlun vegna rekstrarstöðvunar upplýsingakerfa skal endurskoðuð þriðja hvert ár og prófuð fimmta hvert ár[29].

Öryggisendurskoðun

Árlega skal framkvæmt sjálfsmat á upplýsingatækniumhverfi NTÍ sem er mat á umfangi rekstrarins og flækjustigi viðskiptakerfa í samræmi við kröfur FME. Eyðublöð fyrir sjálfsmatið eru aðgengileg á skýrsluskilakerfi FME. Sjálfsmatinu skal skila til FME eigi síðar en í október ár hvert.

Að auki skal innri endurskoðun framkvæma úttekt á upplýsingaöryggisstefnunni og fylgni hennar við leiðbeinandi tilmæli FME nr. 1/2012 um upplýsingakerfi eftirlitsskyldra aðila árlega. Skal sú úttekt taka mið af stærð og umfangi reksturs NTÍ og vera framkvæmd með skipulögðum og markvissum hætti og fylgja almennt þekktri og viðurkenndri aðferðafræði. Niðurstöðum úttektarinnar skal skilað inn til Fjármálaeftirlitsins.[30]

[20] Sbr. grein 10.7.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[21] Sbr. grein 10.7.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[22] Sbr. grein 10.7.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[23] Sbr. grein 10.7.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[24] Sbr. grein 10.7.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[25] Sbr. grein 10.7.6 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[26] Sbr. grein 10.7.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[27] Sbr. grein 10.3.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[28] Sbr. grein 10.8 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[29] Sbr. grein 10.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[30] Sbr. greinar 12.2 og 12.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

5. Útvistun

5.1 Útvistun

NTÍ ber stjórnunarlega ábyrgð á að rekstur upplýsingakerfa uppfylli þær kröfur sem til hans eru gerðar[31]. Þetta á við hvort sem rekstri upplýsingakerfa er útvistað að hluta til eða í heild sinni. Heimilt er að útvista afmörkuðum verkefnum til utanaðkomandi aðila. Hýsingu gagna skal ekki útvistað út fyrir landssteina.

Útvistun þjónustuaðila til þriðja aðila skal ekki heimil nema með samþykki NTÍ.
Þriðja aðila er aldrei heimilt að útvista hýsingu á gögnum NTÍ[32].
Um útvistun til erlendra aðila skal farið skv. kröfum í lið 11.3 í leiðbeinandi tilmælum FME nr. 2/2014 um upplýsingakerfi eftirlitsskyldra aðila.

5.2 Aðkeypt þjónusta

Öryggi upplýsinga skal gætt í samningum við þriðja aðila, s.s. samstarfsaðila, birgja, þjónustuaðila og aðkeypta sérfræðinga. Ákvæði skal vera í samningi um að öll viðskiptafyrirmæli skulu vera skrifleg og vistuð. Með viðskiptafyrirmælum er átt við samskipti sem fela í sér bindandi ákvarðanir milli aðila, s.s. fyrirmæli um framkvæmd ákveðinna viðskipta, staðfestingu á samningum o.s.frv.

Samningar þurfa að ná til eftirfarandi þátta að lágmarki:

- Upplýsingaöryggisstefnunnar í heild.
- Aðgangsstýringar sem notaðar verða.
- Hvaða þjónustu þjónustuaðili skal inna af hendi[33].
- Kröfur NTÍ sem gerðar eru til samningsaðila og undirverktaka.
- Kröfur NTÍ sem gerðar eru til verndar persónugreinanlegum upplýsingum.
- Réttur til að stunda eftirlit með þeirri starfsemi þjónustuaðilans sem samningurinn tekur til.[34]
- Réttur eftirlitsaðila að gögnum á vinnustöð hýsingaraðila[35].
- Ábyrgð varðandi innsetningu og viðhald vélbúnaðar og hugbúnaðar.
- Verkferli við samningslok.
- Ákvæði um heimilt og óheimilt framsal.
- Aðgerðir er varða umhverfisöryggi.
- Trúnaðarsamningur við þjónustuaðila þar sem við á[36].
- Tilnefning ábyrgðaraðila hjá þjónustuaðila.

Tilnefna skal ábyrgðaraðila innan NTÍ, starfsheiti er nægilegt, sem ber ábyrgð á kröfum sem gerðar eru til stofnunarinnar af hálfu FME og þjónustuaðila[37]. Hafi starfsmenn NTÍ ekki nægilega þekkingu (tæknilega eða lagalega) til að gera samning um útvistun skal leita til utanaðkomandi ráðgjafa annars en samningsaðila[38].

[31] Sbr. grein 11.8 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[32] Sbr. grein 11.1-11.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[33] Sbr. grein 11.5.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[34] Sbr. grein 11.5.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[35] Sbr. grein 11.5.4 og 11.5.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[36] Sbr. grein 11.5.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[37] Sbr. grein 11.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[38] Sbr. grein 11.6 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

5.3 Meðhöndlun atvika, frávika og öryggisbrota

Þjónustuaðili skal halda utan um atvik, frávik og öryggisbrot er snúa að rekstri upplýsingakerfa er uppgötvast af hálfu þjónustuaðila. Allar skráningar skulu fara fram í kerfum þjónustuaðila. Ef alvarlegt frávik felur í sér rof á varðveislu, leynd, réttleika og/eða tiltækileika upplýsingakerfa og gagna (t.d. innbrot í upplýsingakerfi, gagnaleki, gagnatap, óvænt rekstrarstöðvun upplýsingakerfa (í heild eða að hluta) sem hefur áhrif á starfsemina) skal þjónustuaðili tilkynna framkvæmdastjóra NTÍ sem fyrst, eða innan 12 klst.

Framkvæmdastjóri ber ábyrgð á því að tilkynningum sé komið áfram til FME innan 24 tíma eftir að frávik uppgötvast. Tilkynningin skal gerð á þar til gert eyðublað í skýrsluskilakerfi FME.[39].

Gæðafulltrúi NTÍ skal kalla eftir skýrslu um atvik, frávik og öryggisbrot hjá þjónustuaðilum á 6 mánaða fresti til staðfestingar á því að þau hafi verið tilkynnt um leið og þau eiga sér stað.

6. Starfsmenn

6.1 Fræðsla og þjálfun í upplýsingaöryggi

Nýjum starfsmönnum skal kynnt upplýsingaöryggisstefna NTÍ ásamt öðrum ferlum sem tengjast upplýsingaöryggi, áhersla skal lögð á að kynna ábyrgð þeirra varðandi upplýsingaöryggi.

Fjalla skal um þjálfun starfsmanna varðandi upplýsingaöryggi við gerð starfsþróunaráætlunar starfsmanna með það að markmiði að tryggja að starfsfólk hljóti fullnægjandi þjálfun og fræðslu varðandi upplýsingaöryggi [40].

6.2 Stefna um að ekkert sé skilið eftir á glámbekk

Starfsmenn skulu ekki skilja eftir viðkvæm gögn eftirlitslaus á skrifborðum eða á öðrum þeim stöðum þar sem óviðkomandi geta komist í þau.
Tölvur skulu vera útbúnar skjávara eða öðrum búnaði sem læsir þeim sjálfkrafa ef engin starfsemi á sér stað í tiltekinn tíma. Starfsmenn skulu ætíð læsa aðgangi að tölvum sínum ef þeir fara frá.

6.3 Fjarvinnsla

Fjarvinnsluaðstaða skilgreinist sem aðstaða er leyfir starfsmanni að tengjast kerfinu gegnum almenningssamskiptatæki, milli vélbúnaðar starfsmanns og upplýsingatæknikerfis stofnunarinnar skal einungis notast við öruggar tengingar. Starfsmönnum NTÍ er leyfilegt að tengjast innri kerfum hennar í gegnum slíka aðstöðu sé búnaður sem nýttur er til tengingarinnar útbúinn uppfærðum vírusvörnum. Fjartengingar starfsmanna skulu skráðar í kerfi þjónustuaðila.

6.4 Meðhöndlun færanlegra gagnamiðla[41]

Sérhver starfsmaður sem hefur færanlegan gagnamiðil (t.d. snjallsíma, spjald- og fartölvu, diskling, snældu, minnislykil, minniskort, færanleg harðdisksdrif, geisladisk, innbyggðar minniseiningar tækjabúnaðar og aðra sambærilega miðla) í fórum sínum ber ábyrgð á öryggi hans.

Færanlega gagnamiðla sem innihalda gögn í leyndarflokknum HÁTT verður að geyma í læstum öryggishólfum, skápum og/eða herbergjum. Bannað er að skilja færanlega gagnamiðla eða annan upplýsingatæknibúnað sem

[39] Sbr. grein 8.5-8.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[40] Sbr. grein 5.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
41 Sbr. grein 5.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

inniheldur gögn í leyndarflokknum HÁTT og MIÐLUNGS, eftir eftirlitslausan á ólæstu vinnusvæði, í ólæstum farartækjum eða á almenningssvæðum. Tölvumiðla sem innihalda gögn í leyndarflokknum MEÐAL og LÁGT má geyma á vinnusvæði starfsmanna.

6.5 Tölvupóst- og netnotkun starfsmanna

NTÍ skal halda verklagsreglu um tölvupóst og netnotkun starfsmanna. Reglurnar skulu taka á eftirfarandi þáttum:

- Heimil og óheimil netnotkun
- Meðferð einkatölvupósts
- Meðferð starfstengds tölvupósts
- Meðferð tölvupósts við starfslok
- Skráningu og skoðun upplýsinga um netvafur

7. Aðgangsstýringar

Uppbygging aðgangsstýringa skal miða að því að stýra aðgangi að upplýsingum og upplýsingakerfum. Aðgangsstýringar starfsmanna, þjónustuaðila og annarra, skal háttað þannig að viðkomandi fái einungis aðgang að þeim upplýsingum sem hann þarf að nota í starfi.

7.1 Heimildagjöf [42]

Aðgangsveitingar fara fram í samræmi við VLR133 um stofnun aðgangs að upplýsinga- og tölvukerfi.
Verklagsreglan skal taka til stjórnunar, úthlutunar, endurskoðunar og afturköllunar aðgangsheimilda að upplýsingakerfum, þ.m.t. færanlegum miðlum og upplýsingavinnslubúnaði. Sá sem veitir aðgang eða framselur heimildir skal vista viðeigandi skjöl í „5.4 Aðgangsstýringar“ í Vörðunni. Aðgangur þjónustuaðila, annarra en rekstraraðila að upplýsingakerfum skal taka mið af mikilvægi hvers verkefnis en skal almennt aldrei veittur til lengri tíma en þrjátíu daga í senn. Skipti starfsmaður um stöðu eða hlutverk innan NTÍ skal laga aðgang hans að kerfum og forritum að hinni nýju stöðu. Hið sama skal gilda um starfsmenn sem hætta þar störfum. Ef utanaðkomandi aðila er veittur aðgangur að upplýsingakerfum skal vera tryggt með skriflegum samningum að kröfur upplýsingaöryggisstefnunnar til öryggis og skjalfestingar séu uppfylltar.[43]

7.2 Stjórnun starfsmannaeinkenna og lykilorða

Ábyrgð á starfsmannaeinkennum og lykilorðum og notkun þeirra er á ábyrgð þess sem skráður er fyrir þeim.

- Starfsmannaeinkenni skulu vera fornafn starfsmanns, skrifað með lágstöfum og engum sérístenskum stöfum. Til að tryggja einkvæmi skal bæta við millinafni eða fyrsta stafi eftirnafns, eða fleirum, ef þörf er á.
- Notkun starfsmanna á sameiginlegum starfsmannaeinkennum er bönnuð.
- Sjálfgefnu lykilorði verður að breyta við fyrstu innskráningu.
- Lykilorði skal breyta á a.m.k. 90 daga fresti.
- Lykilorð skal vera a.m.k. tólf stafir.
- Lykilorð skal innihalda há og lág staf ásamt tölustaf eða tákni.
- Lokað skal fyrir aðgangsorð, ef gerðar eru fleiri en þrjár tilraunir til þess að nota þau án þess að tenging takist.
- Aðgangsorði skal lokað sjálfvirkt hafi það ekki verið notað í 90 daga.

[42] Sbr. grein 5.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[43] Sbr. grein 1.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

- Ekki skal unnt að nota eldra lykilorð að nýju fyrr en eftir a.m.k. fimm umferðir frá því að það var síðast notað.

Starfsmenn skulu vernda lykilorð sín að teknu tilliti til eftirfarandi:

- Lykilorð má aldrei skrifa niður á þann hátt að augljóst sé að um lykilorð sé að ræða.
- Innskráning á vinnustöð má aldrei vera sjálfvirk.
- Notkun á einkenni annars starfsmanns er bönnuð nema í algjörum undantekningartilvikum (sjá næsta lið).
- Starfsmanni er bannað að upplýsa aðra um lykilorð sitt nema í undantekningatilvikum og skal þá skipta um lykilorð eins fljótt og kostur er.

7.3 Aðgangur að kerfum utan stofnunarinnar

Sem hluta af starfi sínu hafa starfsmenn NTÍ aðgang að ýmsum kerfum og upplýsingaveitum (þjóðskrá, fasteignaskrá, o.þ.h.). Gera skal ráðstafanir til þess að stýra aðgangi að viðkomandi kerfum. Ef starfsmenn hafa persónulegan aðgang að kerfum verður að gæta þess að loka fyrir aðganginn þegar þeir hætta eða flytjast til í starfi. Sameiginlegum aðgangi að upplýsingaveitum skal breytt þegar starfsmaður sem hafði aðgang lætur af störfum.

8. Stjórn tölvu- og netkerfa

Í þessum kafla er að finna viðmiðunarreglur varðandi stjórn tölvu- og netkerfa NTÍ.[44]

Rekstur upplýsingakerfa NTÍ er á ábyrgð þjónustuaðila skv. þjónustusamningi milli NTÍ og þjónustusala, reglurnar eru settar fram til þess að tryggja leynd, tiltækileika og réttleika þeirra upplýsinga sem eru í eigu NTÍ. Tryggja skal að fullnægjandi stjórn og stýringar séu til staðar fyrir netkerfi til að tryggja vernd fyrir ógnum og halda uppi öryggi fyrir þau kerfi og hugbúnað sem notar netið, þ.á.m. upplýsingar í flutningi.

8.1 Kerfisstjórn

- Ábyrgðaraðilar kerfa bera ábyrgð á daglegri stjórnun þeirra.
- Við kerfisstjórn skal lögð áhersla á að vinna samkvæmt stöðlum, verklagsreglum og fyrirfram skilgreindum verkferlum.
- Fyrir kerfi í tiltækileikaflokknum HÁTT skv. 4.1.3 skal tryggt að aðgengi sé að þekkingu á viðkomandi kerfi hjá þjónustuaðila.
- Þjónustuaðili skal skrá daglegar aðgerðir og breytingar vegna upplýsingakerfa NTÍ til þess að tryggja rétta verkferla.
- Sérstaka áherslu skal leggja á verklag við innsetningu breytinga er varða öryggi, svo sem leiðréttingar, þjónustupakka o.s.frv.
- Samþykki ábyrgðarmanns kerfis skal liggja fyrir vegna breytinga annarra en minniháttar breytinga sem hafa ekki áhrif á rekstur eða virkni kerfa og/eða hafa áhrif á gögn, áður en breytingar á kerfum eru innleiddar.
- Skrá skal öll þau frávik sem koma upp þegar breytingar á kerfum eru framkvæmdar í raunumhverfi.
- Þjónustuaðili skal sjá um daglegt eftirlit með öllum miðlægum tölvubúnaði.

[44] Sbr. grein 6.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

- Starfsmenn skulu ekki að hafa heimild til breytinga á tölvum sínum nema með leyfi framkvæmdastjóra og kerfisstjóra. Óheimilt er að hlaða niður öðrum hugbúnaði á tölvur en NTÍ leggur til eða samþykkir.

8.2 Vírusvarnir[45]

Tölvur, netþjónar og tölvupóstkerfi skulu vera útbúin vírusvarnarbúnaði og skal hann vera uppfærður reglulega af þjónustuaðila. Notanda er ekki heimilt að breyta virkni eða aftengja vírusvarnarforrit á tölvum. Ef grunur vaknar um að vírus sé á ferli skal starfsmaður tilkynna það án tafar til þjónustuaðila.

8.3 Afritun[46,47]

Gögn skulu vistuð miðlægt. Ekki er tekin ábyrgð á gögnum sem vistuð eru á tölvum og fartölvum nema viðkomandi búnaður falli undir afritunaráætlun. Afrit skulu tekin af öllum gögnum, upplýsingakerfum, forritum og stýrikerfum samkvæmt fyrirfram gerðri áætlun. Endurheimtur gagna og kerfa skal prófa reglulega og niðurstöður skulu skráðar. Afrit skulu ritvarin með þeim hætti að ekki sé mögulegt að eyða eða breyta þeim fyrir mistök á nokkurn hátt[48]. Þegar tekin eru afrit af nýjum gögnum, forritum og stýrikerfum skal sannreyna að afritin séu nothæf. Niðurstöður skulu skráðar. Tryggja skal að afrit séu læsileg til loka geymslutíma[49]. Tryggja skal að afrit verði tekin af stillingum tölvubúnaðar t.d. leiðstjóra (router) og netvirkis (firewall). Tryggja skal að afrit af upplýsingakerfum sem innihalda viðskiptaupplýsingar (allar upplýsingar og gögn um viðskiptavini og stöðu hans gagnvart stofnuninni) séu tiltæk að lágmarki í tvö ár frá uppruna skráningar.[50] Afrit af gögnum skulu vistuð á öruggan hátt jafnt innan sem utan vinnsluhúsnæðis í hæfilegri fjarlægð frá frumgögnum[51]. Afrit skulu tiltæk með skömmum fyrirvara og aðgengi að þeim fyrirhafnarlítið[52] og takmarkað við samþykkta aðila[53]. NTÍ skal viðhafa skjalfesta afritunaráætlun sem skal samþykkt af gæðanefnd. Hún skal a.m.k. innihalda eftirfarandi:

- Lýsingu á markmiðum, framkvæmd og með hvaða hætti nothæfi gagna er staðfest.
- Lýsingu á geymslutíma, staðsetningu afrita og búnaði nauðsynlegum til endurheimta[54].
- Allar kröfur sem gerðar eru til stofnunarinnar um afritunaráætlanir
- Endurheimt gagna.
- Árlegt afrit bókhaldsgagna

8.4 Internet

Þjónustuaðili heildarreksturs upplýsingatæknikerfa ber ábyrgð á að koma á internettengingu fyrir NTÍ gegnum netvirki og viðhalda stýringum fyrir almenningsnet og þráðlaus net til þess að vernda kerfi og notendahugbúnað.[55]Að lágmarki verður netvirki að uppfylla eftirfarandi kröfur:

- Netvirki verður að koma fyrir á aðgangsstýrðu svæði þar sem öll umgengni er skráð..
- Netvirki skal vaktað og prófað eftir fyrirfram skilgreindri áætlun.
- Netvirki skal innihalda búnað sem skynjar innbrotstilraunir.
- Internetnotkun skal vera skráð. Óheimilt er að skoða upplýsingar um netvafur, tengingar og gagnamagn starfsmanns nema fyrir liggi rökstuddur grunur um að hann hafi brotið gegn gildandi lögum og reglum

[45] Sbr. grein 5.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[46] Sbr. grein 4.2.6 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[47] Sbr. grein 9 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[48] Sbr. grein 9.5.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[49] Sbr. grein 9.5.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[50] Sbr. grein 9.2.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[51] Sbr. grein 9.5.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[52] Sbr. grein 9.2.6 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[53] Sbr. grein 9.5.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[54] Sbr. grein 9.2.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[55] Sbr. grein 5.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

eða fyrirmælum framkvæmdastjóra. Sé tilefni skoðunar grunur um refsiverðan verknað skal óska atbeina lögreglu.

- Ábyrgðarmaður þjónustuaðila ber ábyrgð á uppsetningu, stillingum, viðhaldi og daglegri rekstrarstjórnun netvirkis.
- Ábyrgðarmaður þjónustuaðila skal fylgjast með nýjustu upplýsingum um viðhald og rekstur netvirkja.
- Tenging framhjá skilgreindum leiðum skal vera bönnuð.

8.5 Tölvupóstur og önnur samskiptaform

- Notkun tölvupósts er bundin við eiganda hvers einkennis. Tölvupóstföng má því ekki framselja öðrum.
- Upplýsingar sem falla undir leyndarflokkinn „HÁTT" og sendar eru með tölvupósti skal senda dulkóðaðar.
- NTÍ áskilur sér rétt til að meðhöndla tölvupóst sem kemur frá þriðja aðila og uppfyllir ekki öryggiskröfur hennar.
- Flutningur tölvupósts á Internetinu skal fara í gegnum miðlægt netvirki og vírusvörn.
- Miðlægur búnaður skal skanna allan tölvupóst sem kemur inn í kerfið eða fer út úr því, til þess að skynja hvort hann innihaldi vírusa.
- Tölvupóstkerfi skulu stillt á þann hátt að ekki sé mögulegt að eyða tölvupóstum úr grunninum.[56]

8.6 Ytri nettengingar

Þjónustuaðili skal halda lista yfir ytri nettengingar (VPN) NTÍ við þriðja aðila. Eigandi skal skráður fyrir hverja ytri nettengingu. Ytri nettengingum má einungis koma á að fengnu samþykki framkvæmdastjóra.Ytri nettengingar skulu skoðaðar reglulega og vaktaðar af viðkomandi ábyrgðarmanni.

- Ytri nettengingum skal komið þannig á að þær megi einungis nota á þann hátt sem er skilgreindur í þjónustusamningi við viðkomandi þjónustuaðila.
- Regluleg athugun eða skönnun skal framkvæmd á veikleikum netkerfisins.

9. Öflun, þróun, viðhald og niðurlagning upplýsingakerfa

NTÍ er heimilt að úthýsa þróun og viðhaldi upplýsingakerfa og skal taka mið af upplýsingaöryggisstefnu í samningum þess efnis við þjónustuaðila.

Gera skal viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja að sjálfgefið sé að einungis þær persónuupplýsingar séu unnar sem nauðsynlegar eru vegna tilgangs vinnslunnar hverju sinni. Þessi skylda gildir um það hversu miklum persónuupplýsingum er safnað, að hvaða marki unnið er með þær, hversu lengi þær eru varðveittar og aðgang að þeim. Einkum skal tryggja með slíkum ráðstöfunum að það sé sjálfgefið að persónuupplýsingar verði ekki gerðar aðgengilegar ótakmörkuðum fjölda fólks án íhlutunar viðkomandi einstaklings[57].

Allur aðkeyptur hugbúnaður skal skráður hjá framleiðanda áður en hann er tekinn í notkun. Aðgangi að leyfum, leyfislyklum og upphaflegum diskum með hugbúnaði skal stýrt sérstaklega. Þess skal gætt að aðkeyptur hugbúnaður uppfylli öll leyfi varðandi dreifingu og höfundarétt.

[56] Sbr. grein 9.5.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[57] Sbr. 25 gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga

Þar sem þróun hugbúnaðar er í höndum annarra en NTÍ skal gera samninga sem endurspegla upplýsingaöryggisstefnu NTÍ. Gera skal kröfur til þróunaraðila um virka breytingastjórnun og gæðaferli. Einnig skulu gerðar kröfur um aðgangsstýringu að frumkóða forrita.

9.1 Öflun búnaðar[58]

Þegar stofnunin innleiðir nýtt upplýsingakerfi, hvort sem það er hug- og eða vélbúnaður, skal fylgja skilgreindu ferli fyrir innleiðingu kerfisins. Nauðsynlegt er að ferlið innihaldi a.m.k. eftirfarandi:

- Mat á þörfum viðkomandi kerfis.
- Mat á áhrifum nýs upplýsingakerfis á önnur kerfi.
- Greiningu á hugsanlegum áhættum sem fylgja nýju kerfi.
- Greiningu á nauðsynlegum eftirlitsaðgerðum fyrir nýtt kerfi.
- Greiningu á nauðsynlegum aðgerðum til verndar persónugreinanlegra upplýsinga.

9.2 Þróun og kerfisviðhald[59,60]

Þróun og kerfisviðhald fyrir hin ýmsu upplýsingakerfi og fyrir tækniumhverfið í heild verður að taka mið af öryggisþörfum og -stefnu. Það skal vera á hendi ábyrgðaraðila upplýsingakerfa að tryggja viðhald og umsjón upplýsingakerfa þannig að rekstur þeirra sé stöðugur og í samræmi við áætlanir.[61] Samþykki ábyrgðarmanns kerfis þarf að liggja fyrir áður en kerfi er tekið í notkun eða því breytt.[62]

9.2.1 Verndun prófunargagna

Prófunargögn skal vernda sérstaklega. Í þeim tilfellum þar sem prófunargögn eru byggð á raungögnum og/eða persónugreinanlegum gögnum skal gæta þess að þau hljóti sömu vernd og raungögn, þ.á.m. skal tryggja að aðgangur sé aðeins veittur þeim sem þurfi það starfs síns vegna. Gæta skal þess að eyða prófunargögnum (pappír, afritum o.þ.h.) til þess að koma í veg fyrir upplýsingaleka.

9.3 Útgáfu- og breytingastjórnun

Ræða skal um ávinning og möguleg áhrif af breytingum á önnur kerfi/hugbúnað, áður en ákvörðun er tekin um hvort óskað skuli eftir breytingum eða ekki. Þátttakendur í slíkum umræðum geta verið þjónustuaðili, starfsmenn og framkvæmdastjóri eftir atvikum, en gæðafulltrúi ber ábyrgð á að afla staðfestingar frá þjónustuaðila á áhrifum fyrirhugaðra breytinga. Leggja skal mat á áhrif á réttleika, tiltækileika og leynd ásamt áhrifum á virkni upplýsingakerfa og annarra kerfa.

Ef niðurstaðan er sú að breytingar séu æskilegar þarf að leggja mat á kostnað vegna fyrirhugaðra breytinga.

Framkvæmdastjóri skal samþykkja allar breytingar sem hafa í för með sér kostnaðarauka. Ef um hagræðingu eða óbreyttan kostnað er að ræða hefur gæðafulltrúi heimild til að óska eftir fyrirhuguðum breytingum, svo fremi að áhrif á önnur kerfi hafi verið metin. Samþykki framkvæmdastjóra eða gæðafulltrúa skal því ávallt liggja fyrir þegar verkbeiðni vegna stærri breytinga er stofnuð[63]. Vista skal verkbeiðni undir 5.3 Verkbeiðnir á Vörðunni.

[58] Sbr. grein 4.2.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[59] Sbr. grein 4.2.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[60] Sbr. grein 4.2.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[61] Sbr. grein 6.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[62] Sbr. grein 7.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[63] Sjá skilgreiningu á stærri og minni breytingum í liðum a-c í kafla **Error! Reference source not found.**

Þjónustuaðili skal leiðbeina NTÍ ef hann hefur forsendur til að hafa skoðun á framkvæmdinni til breytinga eða hagræðingar. Þjónustuaðili skal beita útgáfustjórnun við þróun hugbúnaðar NTÍ þar sem við á. Þjónustuaðili skal kynna fyrir NTÍ þau aðferðarúrræði sem samþykkt hafa verið.

9.4 Innleiðing kerfa[64]

Þjónustuaðili skal viðhafa sérstakt ferli sem tekur á flutningi kerfa úr þróun yfir í rekstur. Nýtt kerfi eða breytingar skal prófa, sérstaklega skal prófa þá þætti er snúa að öryggi og aðgangsmálum í samvinnu við NTÍ. Gæðafulltrúi skal tilkynna rafrænar skrár eða gagnagrunna til Þjóðskjalasafns Íslands, sem stofnunin mun taka í notkun a.m.k. tveimur vikum áður en ráðgert er að taka kerfið í notkun. Skrá skal öll þau frávik sem koma upp þegar kerfi eru tekin í notkun eða breytingar framkvæmdar í raunumhverfi.

9.5 Niðurlagning á kerfi eða búnaði [65]

Þegar stofnunin leggur niður upplýsingakerfi, hvort sem það er hug- og / eða vélbúnaður, þarf að fylgja GÁT321 um niðurlagningu upplýsingatæknikerfis. Viðhalda skal gátlistanum sem skal að lágmarki innihalda eftirfarandi:

Mat á þörfum viðkomandi kerfis.

- Mat á áhrifum niðurfellingar kerfis á önnur kerfi.
- Tilfærslu nauðsynlegra gagna úr kerfinu.
- Greiningu á hugsanlegum áhættum sem fylgja niðurlagningu kerfis.
- Ferli til enduruppsetningar ef nauðsynlegt.
- Samþykki ábyrgðarmanns kerfis þarf að liggja fyrir áður en kerfinu er lagt.

10. Breytingar

Til breytinga á stefnu þessari þarf samþykki stjórnar.

Stefna þessi var fyrst útgefin í maí árið 2013.

[64] Sbr. grein 4.2.8 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[65] Sbr. grein 4.2.9 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.