Efnisyfirlit

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 og að upplýsingarnar séu réttar og óspilltar.[1]

Upplýsingakerfi, upplýsingar, samskiptaleiðir og áreiðanleiki upplýsinga er mikilvæg forsenda fyrir starfsemi NTÍ. Stjórnun upplýsingaöryggis er því nauðsynleg. Þessi stefna er grundvöllur þeirra ráðstafana sem stofnunin beitir til þess að tryggja öryggi upplýsinga, upplýsingakerfa og samskiptakerfa. Stefnunni skulu fylgja gæðamarkmið á einstökum sviðum upplýsingatækni og frávikaskráning skal fara fram með skipulögðum hætti.[2] Stefnan inniheldur öryggiskröfur til reksturs upplýsingakerfa og tryggir að fyrirliggjandi séu skriflegar lýsingar á öllum verkferlum mikilvægum fyrir rekstur og öryggi upplýsingakerfa.[3] Í slíkum lýsingum skal ábyrgðin á eftirfarandi atriðum, viðvíkjandi rekstri upplýsingatæknikerfa ávallt tryggð:[4]

- Stjórnun
- Öflun búnaðar
- Þróun
- Rekstri
- Kerfisviðhaldi
- Afritun
- Öryggi upplýsinga
- Innleiðingu
- Niðurlagningu kerfa og búnaðar

Öryggisstjórnun og stjórnunarferli beinast að hagsmunum stofnunarinnar. Þess vegna beinist stefnan einnig að:

- Leynd trúnaðarupplýsinga
- Réttleika gagna
- Tiltækileika þjónustunnar

1.1 Ábyrgð

Í ljósi smæðar í yfirbyggingu hjá NTÍ er rekstri, viðhaldi, hýsingu og afritun allra upplýsingakerfa auk hönnunar og þróunar, úthýst til þjónustuaðila innanlands. Stjórn NTÍ ber stjórnunarlega ábyrgð á rekstri og áhættustjórnun 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. 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.

[1] Sbr. inngang í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[2] Sbr. grein 4.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[3] Sbr. grein 4.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[4] Sbr. grein 4.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[5] Sbr. grein 3.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

1.2 Afmörkun

Upplýsingaöryggisstefnan og viðmið sem henni fylgja ná til þjónustu, eigna, upplýsinga og búnaðar sem stofnunin hefur umsjón með eða felur öðrum að sjá um í sínu nafni. Þetta skjal lýsir upplýsingaöryggisstefnu NTÍ eins og hún er samþykkt af stjórn NTÍ og nær til allrar starfsemi, starfsmanna og upplýsingakerfa hennar. Með upplýsingakerfum er átt við þau vélrænu kerfi sem koma að vinnslu upplýsinga ásamt öllum tengingum að, frá og á milli þeirra.[6]

1.3 Skilgreining öryggis

Samkvæmt þessari stefnu er „upplýsingaöryggi“ skilgreint sem kerfi þeirra aðgerða og ráðstafana sem stofnunin notar til þess að standa vörð um leynd, réttleika og tiltækileika gagna og upplýsingakerfa.

- 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 og öryggi

2.1 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.
- 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.

[6] Sbr. grein 1.2 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 VTÍ.

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. Flokkun og stjórnun eigna

3.1 Listi yfir eignir

Halda skal lista yfir mikilvægar eignir sem við koma úrvinnslu, geymslu og miðlun upplýsinga, rekstraröryggi stofnunarinnar, ásamt upplýsingum um staðsetningu eignanna og lýsingu á þeim. Meðal þessara eigna eru vélbúnaður, hugbúnaður, gagnaskrár, þjónusta og húsnæði. Þessi skráning skal fara fram í samvinnu við þjónustuaðila og vera uppfærð árlega.[9]
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:

3.1.1 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 NTÍ án leyfis.
LÁGT	Almennar upplýsingar. Upplýsingar sem geta ekki skaðað ímynd NTÍ 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.

3.1.2 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.

3.1.3 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.

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

3.2 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 ásamt því að hafa skal eftirlit með þeim. Stofnunin skal ákveða viðmið fyrir ásættanlega áhættu tengda notkun upplýsingatækni m.t.t. starfssviðs og flækjustigs viðkomandi aðila. Í því sambandi þarf jafnframt að endurskoða viðmiðin með reglubundnum hætti og greina áhættu af rekstri upplýsingakerfa.[10] 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.[11] Niðurstaða áhættumatsins skal skjalfest og samþykkt ásamt tillögum til úrbóta þar sem þörf er á eftirfylgni.[12] Taka skal ákvörðun um hvort þörf sé fyrir frekari öryggisráðstafanir en tilgreindar eru í upplýsingaöryggisviðmiðum samhliða áhættumatinu.

Upplýsingatæknikerfi er sá hluti rekstraráhættu sem er hvað viðkvæmastur fyrir rekstraráhættu.[13] 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. Rík áhersla skal lögð á skjalfestingu krafna hvað varðar öryggismál og afritun. Upplýsingaöryggisstefna skal kveða á um kröfur til meðferðar á upplýsingatengdum eignum og Viðbragðsáætlun upplýsingatæknikerfa (VLR238) skal skilgreina hvaða viðbrögð hafa verið ákveðin fyrir truflanir á upplýsingakerfum til að þau valdi sem minnstri truflun á rekstrinum.[14] Þjónustuaðili í upplýsingatækni sem samið er við um heildarrekstur upplýsingatæknikerfa skal að lágmarki uppfylla ISO27001 upplýsingastjórnunarstaðalinn.[15]

4. Starfsmenn og öryggi

4.1 Listi yfir aðila

Skilgreining á aðilum sem hafa hlutverk er tengist upplýsingaöryggi hjá NTÍ:

- *Starfsmenn* eru allir þeir sem eru launþegar hjá stofnuninni.
- *Stjórn* er skipuð skv. lögum 55/1992 um NTÍ.
- *Þjónustuaðilar* eru ekki fastráðnir starfsmenn NTÍ en veita henni þjónustu samkvæmt samningi. Þjónustuaðilar skiptast í þrjá flokka:
    - *Þjónustuaðili 1*: Þjónustuaðilar í flokki 1 skulu hafa samning við NTÍ þar sem verksvið og ábyrgð þeirra er skilgreind ásamt skilgreindum aðgangi að rými og/eða kerfum NTÍ. Þjónustuaðilum í þessum flokki er treyst til að vinna án viðvarandi eftirlits starfsmanns. Dæmi um þjónustuaðila 1 eru aðilar sem sjá um ræstingu, öryggisverðir og starfsmenn þjónustuaðila sem sér um heildarrekstur upplýsingaöryggiskerfa.
    - *Þjónustuaðili 2* : Hefur aðgang að almennu vinnusvæði starfsmanna en verður að vera í fylgd og undir eftirliti starfsmanns. Starfsmenn skulu hafa eftirlit með því að vinna þjónustuaðila 2 sé

[10] Sbr. grein 2.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[11] Sbr. grein 2.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[12] Sbr. grein 2.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[13] Sbr. 95. lið leiðb. tilmæla FME nr. 1/2011
[14] Sbr. gr. 2.2.7 í áhættustýringarstefnu NTÍ
[15] Sbr. gr. 2.2.7 í áhættustýringarstefnu NTÍ

í samræmi við verkbeiðni og reglur NTÍ. Dæmi um þjónustuaðila 2 eru matsmenn og endurskoðendur.
    - *Þjónustuaðili 3* : Hefur aðeins aðgang að almennu rými og fær aðgang að almennu vinnusvæði starfsmanna undir eftirliti starfsmanns. Dæmi um þjónustuaðila 3 eru sendlar, viðgerðaraðilar og birgjar.
- *Gestir eru þeir sem eru gestir einhvers starfsmanns NTÍ.*

Stefna þessi gildir um alla ofangreinda hópa.

4.1.1 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.*
- *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.*
- *Réttur eftirlitsaðila að gögnum á vinnustöð hýsingaraðila.*
- *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.*
- *Tilnefning ábyrgðaraðila hjá þjónustuaðila.*

Tilnefna skal ábyrgðaraðila innan NTÍ sem ber ábyrgð á kröfum sem gerðar eru til stofnunarinnar af hálfu FME og þjónustuaðila.

Hafi starfsmenn NTÍ ekki nægilega þekkingu (tæknilega eða lagalega) til að gera samning um útvistun skal leita til utanaðkomandi ráðgjafa annars en samningsaðila.

4.1.2 Ferilkönnun

NTÍ skal gera ráðstafanir til að ganga úr skugga um heiðarleika og áreiðanleika nýrra starfsmanna fyrir ráðningu. Í sumum tilfellum getur reynst nauðsynlegt að framkvæma ferilkönnun vegna þjónustuaðila 1. Með starfsumsókn skal alltaf óskað eftir meðmælum og upplýsingum um menntun og reynslu.

Um trúnaðaryfirlýsingar starfsmanna fer eins segir í Mannauðsstefnu (SSK162). Samningar við þjónustuaðila 1 og 2 skulu innihalda trúnaðaryfirlýsingu. Þó er leyfilegt að sleppa trúnaðaryfirlýsingu við þjónustuaðila 3 ef þjónusta þeirra krefst þess ekki.

4.2 Fræðsla og þjálfun í upplýsingaöryggi[16]

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.

4.3 Meðhöndlun atvika, frávika og öryggisbrota

NTÍ gerir greinarmun á atvikum, frávikum og öryggisbrotum með eftirfarandi hætti: Atvik teljast ófyrirsjáanleg atvik og/eða rekstrarrof, til frávika teljast aðgerðir eða atburðir þar sem ekki er farið skv. verklagsreglum og stefnum, án þess að vísbendingar liggi fyrir að um ásetning sé að ræða. Öryggisbrot eru brot á verklagsreglum og stefnum sem verða ítrekað, eða af ásetningi.

Öll atvik, frávik og öryggisbrot sem verður vart við hjá NTÍ og hafa áhrif eða geta haft áhrif á leynd, réttleika eða tiltækileika skal skrá á frávikalista á innraneti og fylgja VLY144 um Frávik, forvarnir og úrbætur. Öll öryggisbrot skal tilkynna til framkvæmdastjóra NTÍ strax og þeirra verður vart. Um meðferð brota skal fara skv. reglum fjármálaráðuneytisins: http://www.fjarmalaraduneyti.is/starfsmenn-rikisins/yfirlit/starfsaevin/starfsskyldur/

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 atburðurinn 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. Tilkynningin skal gerð á þar til gert eyðublað í skýrsluskilakerfi FME.[17].

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.

4.4 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. Fjartengingar starfsmanna skulu skráðar í kerfi þjónustuaðila.

5. Umhverfisöryggi

Umhverfisöryggi lýsir aðgerðum er miða að því að tryggja aðgengi að byggingum þar sem ein eða fleiri einingar NTÍ eru hýstar.

Innan bygginganna eru skilgreind eftirfarandi *svæði* og skal inngangsvarsla vera í samræmi við skilgreiningu svæðanna eða eftir því sem við á:

A svæði	Þar eru allir miðlarar, netbúnaður og afritunarbúnaður vistaður. Aðgangur heimilaður af hýsingaraðila samkvæmt samningi. Halda skal skrá yfir aðgangsstýringar svæðisins.

[16] Sbr. grein 5.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[17] Sbr. grein 8.5-8.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

B svæði	Tengiskápur og skjalageymsla. Einungis starfsmenn hafa aðgang að viðkomandi svæðum og hafa leyfi til þess að gefa aðgang. Takmarka skal utanaðkomandi aðgang eins og mögulegt er.
C svæði	Svæði starfsmanna NTÍ. Einungis starfsmenn hafa aðgang að viðkomandi svæðum og hafa leyfi til þess að gefa aðgang.
D svæði	Afgreiðsla þar sem almenningur hefur aðgang.
E svæði	Sameign húss.

5.1 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.

5.2 Öryggi tækjabúnaðar og gagna[18]

Gera skal ráðstafanir til þess að verja allan helsta tækjabúnað og gögn gegn skemmdum t.d. af völdum áfalla, misnotkunar, óheimilum aðgangi, óheimilla breytinga, skemmdarverka, þjófnaðar, eldsvoða, reyks, vatns og rafmagnstruflana[19]. 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.[20] Aðgangur að helstu rafmagns- og fjarskiptalögnum skal varinn sérstaklega.

5.2.1 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 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.

5.2.2 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. Ef harðir diskar, geisladiskar og disklingar skemmast skal sjá til þess að þeir verði algjörlega eyðilagðir áður en þeim er hent.

5.3 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

[18] Sbr. grein 4.2.7 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[19] Sbr. grein 5.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[20] Sbr. skilgreiningar í markmiðum og tilgangi upplýsingaöryggisstefnunnar

- 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.

6. Stjórn tölvu- og netkerfa

Í þessum kafla er að finna viðmiðunarreglur varðandi stjórn tölvu- og netkerfa NTÍ.[21]

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.

6.1 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. lið 3.1.3 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.
- 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.
- Útvistun þjónustuaðila til þriðja aðila skal ekki heimil nema með samþykki NTÍ.
- Þriðja aðila er aldrei heimilt að útvista hýsingu á gögnum NTÍ.
- Um útvistun til erlendra aðila skal farið skv. kröfum í lið 11.3 í leiðbeinandi tilmælum FME nr. 2/2014 um upplýsingakerfi eftirlitsskyldra aðila.

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

6.2 Vírusvarnir[22]

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.

6.3 Afritun[23,24]

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, forritum og stýrikerfum samkvæmt fyrirfram gerðri áætlun. Afritum skulu gefin einkvæm númer eða heiti. Endurheimtur gagna og kerfa skal prófa a.m.k. árlega. Slíkar prófanir skulu skráðar. Afrit skulu ritvarin með þeim hætti að ekki sé mögulegt að eyða eða breyta þeim fyrir mistök á nokkurn hátt. 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. 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.[25] Afrit af gögnum skulu vistuð á öruggan hátt jafnt innan sem utan vinnsluhúsnæðis í hæfilegri fjarlægð frá frumgögnum. Afrit skulu tiltæk með skömmum fyrirvara og aðgengi að þeim fyrirhafnarlítil og takmörkuð við samþykkta aðila. 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 að endurheimtaafritunaráætlun
- Allar kröfur sem gerðar eru til stofnunarinnar um afritunaráætlanir
- Endurheimt gagna.
- Árlegt afrit bókhaldsgagna

6.4 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. Niðurstaðan á þessu stigi getur verið sú að halda áfram með umræðu í samþykktarferli eða hætta við fyrirhugaðar breytingar.

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

[22] Sbr. grein 5.4 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[23] Sbr. grein 4.2.6 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[24] Sbr. grein 9 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[25] Sbr. grein 9.2.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

áhrif á önnur kerfi hafi verið metin. Samþykki framkvæmdastjóra eða gæðafulltrúa skal því ávallt liggja fyrir þegar verkbeiðni vegna stærri breytinga er stofnuð[26]. Vista skal verkbeiðni undir 1.1.06, úrbætur á Vörðunni.

Þjónustuaðili skal leiðbeina verkbeiðanda 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.
Þjónustuaðilar skulu viðhafa kerfisskráningu fyrir kerfi og búnað í þjónustu. Skráningin skal að lágmarki beina athygli að eftirfarandi færslum í kerfinu:

a) Stærri breytingum á búnaði (vél- og hugbúnaði) í víðnets- og rekstrarumhverfi NTÍ. Til stærri breytinga teljast allar breytingar sem hafa áhrif á virkni kerfis og gögn. Þar má t.d. nefna aðgerðir sem hafa í för með sér fjölgun eða fækkun aðgerða, þróun á tilteknum aðgerðum, o.s.frv. Stærri breytingar krefjast samþykkis eiganda.
b) Minni breytingum á rekstrarumhverfi NTÍ. Þær hafa ekki áhrif á rekstur eða virkni kerfa og/eða áhrif á gögn. Til minni breytinga teljast t.d. kerfisuppfærslur frá framleiðanda staðlaðs hug- og vélbúnaðs. Minni breytingar krefjast ekki samþykkis eiganda.
c) Rekstaratvikum (atvik, frávik og öryggisbrot) og úrlausnum við þeim, hvort sem atvikið leiddi til þjónusturofs eða ekki.

Að lágmarki skal skrá eftirfarandi:

Fyrir stærri breytingar:

- Á hvaða búnaði breyting var gerð og eðli hennar (nýtt, uppfært, tekið burt).
- Ástæðu breytingar.
- Áhættumat.
- Virkjun breytingar.
- Afturhvarfsáætlun.
- Niðurstöðu.
- Samþykkt fyrirhugaðra breytingar af eiganda.
- Staðfesting á áhrifum fyrirhugaðra breytinga af gæðastjóra.
- Minni breytingar.
- Á hvaða búnaði breyting var gerð og eðli hennar (nýtt, uppfært, tekið burt).
- Upplýsa skal eiganda um breytingarnar eftir því sem kostur er.

Rekstraratvik:

- Umfang atviks.
- Hverju var breytt og eðli þeirra.
- Ástæðu.
- Úrlausn.

Einnig skal skrá eftirfarandi atriði:

- Ræsingu og stöðvun kerfa.
- Uppsetningu nýs vélbúnaðar.

[26] Sjá skilgreiningu á stærri og minni breytingum í liðum a-c í kafla 6.4

- Innsetningu nýs kerfis.

6.5 Meðhöndlun tölvumiðla[27]

Sérhver starfsmaður sem hefur tölvumiðil (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. Gerður er greinarmunur á ferns konar starfsemi er varðar tölvumiðla: Stjórnun, viðhaldi, endurnýtingu og eyðileggingu miðla.

Stjórnun:
Tölvumiðla sem innihalda gögn í leyndarflokknum HÁTT verður að geyma í læstum öryggishólfum, skápum og/eða herbergjum. Bannað er að skilja tölvumiðla eða annan upplýsingatæknibúnað sem 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 C.

Viðhald:
Til þess að koma í veg fyrir eyðileggingu miðla vegna aldurs eða breytinga á tækni skal flytja gögn á milli miðla eftir þörfum eða eins og breytingar á tækni gefa tilefni til.

Endurnýting:
Tryggja verður að gögnum verði eytt út af gagnamiðlum sem eru endurnýttir.

Eyðilegging:
Ef tölvumiðlar sem innihalda gögn í leyndarflokkunum HÁTT og MIÐLUNGS eru ekki lengur í notkun eða þeim hefur verið fargað, skulu gögnin sem þeir innihalda gerð ólæsileg áður. Öllum segulmiðlum og geisladiskum skal eytt undir eftirliti þjónustuaðila.

6.6 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.[28]

6.6.1 Internetstjórnun

Að lágmarki verður netvirki að uppfylla eftirfarandi kröfur:

- Netvirki verður að koma fyrir á **svæði A**.
- Netvirki skal vaktað og prófað eftir fyrirfram skilgreindri áætlun.
- Netvirki skal innihalda búnað sem skynjar innbrotstilraunir.
- Internetnotkun skal vera skráð. NTÍ áskilur sér rétt til þess að vakta Internetnotkun starfsmanna samkvæmt viðeigandi lögum og reglum.
- Tenging framhjá skilgreindum leiðum skal vera bönnuð.
- Ábyrgðarmaður ber ábyrgð á uppsetningu, stillingum, viðhaldi og daglegri rekstrarstjórnun netvirkis.
- Ábyrgðarmaður skal fylgjast með nýjustu upplýsingum um viðhald og rekstur netvirkja.

27 Sbr. grein 5.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

28 Sbr. grein 5.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

6.7 Tölvupóstur og önnur samskiptaform

Reglum um tölvupóst og internetnotkun er ætlað að tryggja að jafnvægi ríki annars vegar á milli hagsmuna NTÍ af því að geta fylgst með því að sá hug- og vélbúnaður sem stofnunin leggur til sé nýttur í þágu stofnunarinnar og hins vegar hagsmuna starfsmanna af því að njóta eðlilegs einkalífsréttar á vinnustað.

6.7.1 Skilgreiningar

Í reglum þessum hafa eftirfarandi orð merkingu sem hér greinir:

1. Einkatölvupóstur, merkir tölvupóst sem starfsmaður NTÍ sendir eða móttekur með vél- eða hugbúnaði stofnunarinnar, og lýtur einungis að einkamálefnum hans en varðar hvorki hagsmuni NTÍ né starfsemi hennar.

2. Netnotkun, merkir notkun starfsmanns á þeim hug- og vélbúnaði sem NTÍ lætur honum í té, t.d. til að vafra um netið, til að taka við og senda tölvupóst eða til snarspjalls (msn).

3. Netvöktun, merkir viðvarandi eða reglubundna söfnun upplýsinga um netnotkun starfsmanna.

4. Tölvukerfi, tekur m.a. til tölvupóstkerfis og þess hug- og vélbúnaðar sem þarf til að tengjast netinu.

6.7.2 Netnotkun

Starfsmönnum NTÍ er heimilt að nýta tölvukerfi NTÍ bæði til að vafra um netið og taka við og senda tölvupóst, enda séu slík einkanot í hófi.

Eftirfarandi netnotkun er starfsmönnum óheimil:

1. Sending dreifibréfa sem er óviðkomandi starfsemi NTÍ, t.d. keðjubréfa eða dreifibréfa vegna sölumennsku eða safnana.

2. Sjálfvirk áframsending tölvupósts úr tölvupóstkerfi NTÍ, t.d. á einkatölvupóstfang starfsmanns hjá netþjónustuaðila, nema slíkt sé gert með leyfi framkvæmdastjóra.

3. Sending efnis sem er ólöglegt, ósiðlegt, illgjarnt, hótandi, hrottafengið, ærumeiðandi, hatursfullt, hvetur til ólöglegs athæfis eða getur gefið tilefni til skaðabótakröfu á hendur stofnuninni. Þetta gildir bæði um efni tölvupósts og efni viðhengja. Sama á við um notkun efnis sem hætta er á að geti verið vírussmitað.

4. Notkun á tölvukerfi stofnunarinnar til að nálgast ósiðlegt efni á netinu, s.s. klám, og/eða skoða eða vista slíkt efni í tölvukerfi NTÍ eða á öðrum miðli.

5. Vegna þess skaða sem tölvuveirur geta valdið á gögnum í tölvukerfi er starfsmönnum óheimilt að opna tölvupóst með viðhengi frá óþekktum sendanda eða að opna viðhengi með tölvupósti sem auðkennd eru með endingum s.s. .exe, .vba, .sit eða .zip nema þeir séu þess fyrirfram fullvissir að slíkt sé óhætt.

6. Notkun á tölvukerfi stofnunarinnar til að nálgast og/eða hala niður mjög stórum skrám á netinu, s.s. kvikmyndum og tónlist, og vista í tölvukerfi NTÍ.

6.7.3 Meðferð tölvupósts

Einkatölvupóstur

Óheimilt er að skoða einkatölvupóst starfsmanna. Til viðmiðunar um það hvort um slíkan póst sé að ræða skal m.a. litið til þess hvort hann sé:

1. Auðkenndur sem einkamál í efnislínu (e. subject), eða að öðru leyti þannig að augljóst sé að einungis sé um einkamálefni er að ræða.

2. Vistaður í sérstakri möppu (e. folder) á vinnusvæði starfsmanns í tölvupóstkerfinu sem er auðkennd þannig eða ef af öðru má ráða að um einkamál sé að ræða.

Þrátt fyrir ákvæði 1. mgr. er heimilt að skoða einkatölvupóst starfsmanna ef brýna nauðsyn ber til, s.s. vegna tölvuveiru eða sambærilegs tæknilegs atviks. Slíka skoðun má aðeins framkvæma að fyrirmælum framkvæmdastjóra. Ávallt skal þó fyrst leita eftir samþykki starfsmanns ef þess er kostur. Enda þótt starfsmaður neiti að veita slíkt samþykki skal veita honum færi á að vera viðstaddur skoðunina. Geti starfsmaður ekki verið viðstaddur skoðunina sjálfur skal veita honum færi á að tilnefna annan mann í sinn stað. Ef ekki reynist unnt að gera starfsmanni viðvart um skoðunina fyrirfram skal honum gerð grein fyrir henni strax og hægt er. Starfsmaður á rétt á vitneskju um hver eða hverjir hafa skoðað einkatölvupóst hans.

Starfstengdur tölvupóstur

Starfstengdan tölvupóst má skoða ef:

1. Nauðsyn ber til vegna lögmætra hagsmuna NTÍ, s.s. til að finna gögn þegar starfsmaður er forfallaður, hefur látið af störfum eða grunur hefur vaknað um misnotkun eða brot í starfi.

2. Nauðsyn ber til vegna tilfallandi atvika, s.s ef endurbætur, viðhald á tölvukerfum eða eftirlit með þeim leiða óhjákvæmilega til þess að tölvupóstur opnast eða þarf að opna.

Skoðun á tölvupósti skv. 1. mgr. má aðeins framkvæma að fyrirmælum framkvæmdastjóra, en ávallt skal kappkostað að leita eftir samþykki viðkomandi starfsmanns og veita honum kost á að vera viðstaddur skoðunina. Geti starfsmaður ekki verið viðstaddur skoðunina sjálfur skal veita honum færi á að tilnefna annan mann í sinn stað. Þetta á þó ekki við ef brýnir hagsmunir mæli gegn því að beðið sé eftir starfsmanni, s.s. í því tilviki þegar um er að ræða alvarlega bilun í tölvukerfinu, og ekki verði talið að einkalífshagsmunir starfsmanns vegi þyngra. Ríki um það vafi hvort svo sé má ekki skoða tölvupóstinn nema honum hafi fyrst verið veittur kostur á að vera viðstaddur skoðunina. Starfsmaður á rétt á vitneskju um hver eða hverjir hafa skoðað tölvupóst hans.

6.7.4 Um meðferð tölvupósts við starfslok o.fl.

Starfsmanni ber að eyða einkatölvupósti sínum þegar hann lætur af störfum. Geri hann það ekki verður slíkum pósti eytt einum mánuði eftir að starfsmaður hefur látið af störfum. Við starfslok er óheimilt að framsenda tölvupóst úr netfangi viðkomandi starfsmanns á netfang framkvæmdastjóra eða annarra starfsmanna. Ekki er heimilt að taka umrætt netfang í notkun fyrr en að liðnum 6 mánuðum frá starfslokum.

Við starfslok skal starfsmanni gefinn kostur á að taka afrit af einkatölvupósti.

Þegar starfsmaður lætur af störfum skal netfangi hans lokað án tafar. Þá skal og slökkva á sjálfkrafa framsendingu tölvupósts sem berst á netfang hans hjá NTÍ. Samtímis skal stilla tölvupóstkerfi stofnunarinnar þannig að allur tölvupóstur á það netfang verði framvegis endursendur ásamt ábendingu um að starfsmaðurinn hafi látið af störfum og á hvaða netfang stofnunarinnar nú eigi að senda erindið. Þar skal og tilgreina nýtt netfang starfsmannsins, óski hann eftir að það verði látið fylgja með.

Starfsmönnum er óheimilt að auðkenna eða vista tölvupóst sem eingöngu varðar starfsemi NTÍ þannig að ætla megi að um einkatölvupóst sé að ræða. Tölvupóst, sem eingöngu varðar starfsemi NTÍ, skulu starfsmenn án tafar færa undir viðhlítandi mál í málaskrá stofnunarinnar.

6.7.5 Skoðun netvafurs

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

6.7.6 Notkun Nets og tölvupósts

Þegar um er að ræða starfstengdan tölvupóst skulu starfsmenn vanda frágang, stafsetningu og málfar. Starfsmenn skulu hafa í huga að samskipti um netið eru ekki með öllu örugg og oft hentar tölvupóstur ekki fyrir viðkvæm gögn eða trúnaðarupplýsingar, einkum vegna hættu á að óviðkomandi geti komist yfir og lesið tölvupóstinn einhvers staðar á leið hans eða hann glatist.

Vegna þeirrar hættu að tölvupóstur berist í rangar hendur skal allur útsendur tölvupóstur frá NTÍ hafa að geyma staðlaðan niðurlagstexta þar sem kveðið er á um að pósturinn kunni að innihalda trúnaðarupplýsingar sem ekki eru ætlaðar lesanda ásamt leiðbeiningum um hvernig hann skuli bregðast við ef svo háttar til.

- 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.[29]

6.8 Ytri nettengingar

Ef ákveðið verður að koma á ytri nettengingum skal halda lista yfir nettengingar NTÍ við þriðja aðila. Eigandi skal skráður fyrir hverja ytri nettengingu. Ytri nettengingum má einungis koma á að fengnu samþykki gæðanefndar og ábyrgðarmanns að undangengnu skriflegu áhættumati ef þess er talið þörf.

- 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 af gæðanefnd.
- Regluleg athugun eða skönnun skal framkvæmd á veikleikum netkerfisins.

6.9 Stefna um notkun dulkóðunar

Við notkun dulkóðunar skal gæta þess að uppfylla lög sem kunna að ná yfir og takmarka notkun dulkóðunar. Þetta á sérstaklega við um skjöl eða gögn sem send eru erlendis þar sem önnur lög kunna að vera í gildi. Ef ákveðið verður að nota dulkóðun sem ráðstöfun gegn uppljóstrun eða upplýsingaleka skal hafa eftirfarandi í huga:

- Hvaða háttur skal hafður á notkun dulkóðunar.
- Hvaða háttur skal hafður á umsjón með lyklum.
- Hver fer með umsjón lykla.
- Hvaða ráðstafanir skal gera ef lyklar týnast.

[29] Sbr. grein 9.5.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

6.10 Þráðlaus net

Þráðlaus net eru leyfileg hjá NTÍ og skulu þau vera aðgangsstýrð á sem öruggastan máta og ekki minna öryggisstig en WPA2.

7. Aðgangsstýringar

Uppbygging aðgangsstýringa skal miða að því að stýra aðgangi að upplýsingum og upplýsingakerfum. Virk breytingastjórnun aðgangs er stór hluti af upplýsingaöryggi NTÍ. Aðgangsstýringar starfsmanna, þjónustuaðila og annarra, skal háttað þannig að viðkomandi fái einungis aðgang að þeim upplýsingum sem hann þarf að nota í starfi.

Eftirfarandi telst til upplýsinga- og tölvukerfa:

- Gögn og gagnaskrár.
- Forrit.
- Hlutar tækniumhverfisins, stýrikerfi, net, vélbúnaður, þjónar, vinnslustöðvar, jaðartæki, tölvur og beinar.

7.1 Heimildagjöf [30]

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 skrá alla heimildagjöf á skýran og skipulegan hátt undir flokki „5.6 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. Gæðafulltrúi skal halda lista yfir allar aðgangsheimildir starfsmanna í öllum kerfum. Ef utanaðkomandi aðila er veittur aðgangur að upplýsingakerfum skal vera tryggt með skriflegum samningum að kröfur upplýsingaöryggisstefnunnar til öryggis og skjalfestingar séu uppfylltar.[31]

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 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.

[30] Sbr. grein 5.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[31] 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.

7.4 Öryggisendurskoðun

Árlega skal gæðanefnd framkvæma 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.[32]

8. Öflun, þróun og viðhald upplýsingakerfa

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

Allur aðkeyptur hugbúnaður skal skráður hjá framleiðanda áður en hann er tekinn í notkun. Öll leyfi skulu geymd á einum stað undir flokki „5.2 Hugbúnaður“ í Vörðunni og skal ábyrgð fyrir geymslu og umsjón leyfa vera falin gæðafulltrúa. 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.

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.

[32] Sbr. greinar 12.2 og 12.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

8.1 Öflun búnaðar[33]

Þegar stofnunin innleiðir nýtt upplýsingakerfi, hvort sem það er hug- og eða vélbúnaður, þarf að skilgreina 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.

8.2 Þróun og viðhald[34,35]

Þróun og viðhald 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.[36] Samþykki ábyrgðarmanns kerfis þarf að liggja fyrir áður en kerfi er tekið í notkun eða því breytt.[37]

8.2.1 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[38]. Gæta skal þess að eyða prófunargögnum (pappír, afritum o.þ.h.) til þess að koma í veg fyrir upplýsingaleka.

8.3 Innleiðing kerfa[39]

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. Tilkynna skal 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.

8.4 Niðurlagning á kerfi eða búnaði [40]

Þegar stofnunin leggur niður upplýsingakerfi, hvort sem það er hug- og / eða vélbúnaður, þarf að skilgreina ferli fyrir niðurlagningu kerfisins. Nauðsynlegt er að ferlið innihaldi a.m.k. 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.

[33] Sbr. grein 4.2.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[34] Sbr. grein 4.2.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[35] Sbr. grein 4.2.5 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[36] Sbr. grein 6.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[37] Sbr. grein 7.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[38] Sbr. grein 7.3 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[39] Sbr. grein 4.2.8 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[40] Sbr. grein 4.2.9 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

- Samþykki ábyrgðarmanns kerfis þarf að liggja fyrir áður en kerfinu er lagt.

9. Rekstrarstöðvun upplýsingakerfa

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.[41]

9.1 Viðbragðsáætlun[42]

Áhættumat (sem lýst er í kafla 2.2) skal gefa vísbendingu um það hvaða upplýsingakerfi eru nauðsynleg fyrir áframhaldandi starfsemi.[43] Viðbragðsáætlun skal gerð til að tryggja áframhald úrvinnslu í þeim kerfum sem teljast mikilvægust samkvæmt áhættumati og falla undir tiltækileikaflokkinn „HÁTT“. Viðbragðsáætlunin skal taka til þeirra einstöku þátta sem geta brugðist og til hvaða viðeigandi ráðstafana skal grípa. Viðbragðsáætlunin skal miða að því að koma af stað og vakta aðgerðir sem miða að því að standa vörð um órjúfanleika upplýsingakerfa.

Viðbragðsáætlunin skal innihalda eftirfarandi:

- Yfirsýn yfir upplýsingakerfin sem tilheyra áætluninni.
- Lýsingu á áfallalausnum.
- Skýr viðmið um hvenær skuli gripið til áfallalausna.
- Ásættanleg tímamörk rekstrarstöðvunar áður en gripið er til áfallalausna.
- Skýr viðmið um hvenær ræsa skal neyðarhóp (framkvæmdastjóri, og/eða gæðafulltrúi ásamt fulltrúa þjónustuaðila).
- Verkferlum til að koma rekstri upplýsingakerfa aftur í gang.
- Yfirsýn yfir ábyrgðarsvið og gangsetningarferla áfallalausna.
- Upplýsingagjöf til stjórnar, starfsmanna, viðskiptamanna og annarra aðila sem vitneskju þurfa að hafa um rekstrarstöðvun.
- Ef endurheimtaraðgerðir hafa í för með sér notkun afrita skulu eftirfarandi atriði skilgreind:
    - 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.[44]

Viðbragðsáætlun vegna rekstrarstöðvunar upplýsingakerfa skal endurskoðuð annað hvert ár og prófuð fimmta hvert ár.

10. Breytingar

Til breytinga á stefnu þessari þarf samþykki stjórnar. Stefnan skal endurskoðuð a.m.k. árlega.

[41] Sbr. grein 10.1 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[42] Sbr. grein 10 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[43] Sbr. grein 10.2 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.
[44] Sbr. grein 10.8 í leiðbeinandi tilmælum FME um upplýsingakerfi eftirlitsskyldra aðila.

Upplýsingaöryggisstefna NTÍ

Stefna þessi var fyrst útgefin í maí árið 2013.