Öryggisstefna Heilbrigðisstofnunar Suðurnesja í upplýsingatækni

Samþykkt í framkvæmdastjórn HSS 18. apríl 2007

Unnið af nefnd um öryggi í upplýsingatækni skipaðri af framkvæmdastjórn HSS í febrúar 2007

Agnar Guðmundsson formaður
Auður Harðardóttir
Hildur Helgadóttir
Sigurður Árnason
Sigurjón Kristinsson

Efnisyfirlit

Tilgangur

Tilgangurinn með þessu skjali er:

Að tryggja að starfsemi Heilbrigðisstofnunar Suðurnesja sé aldrei í hættu.

Tilgreina hlutverk og ábyrgðir fyrir ýmsum atriðum í daglegu starfi HSS.

Koma á stöðluðum verkferlum til að hjálpa til við ofangreind atriði.

Upplýsingaöryggisstefnunni er ætlað að tryggja að farið sé að lögum, þ.m.t. lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

Umfang

Umfang þessa skjals er allt frá ráðningum starfsmanna upp í daglegan rekstur HSS. Skjalið fjallar um upplýsingakerfi Heilbrigðisstofnunnar Suðurnesja og hvernig best sé að tryggja öryggi þess við daglega vinnslu.

Ábyrgð

Framkvæmdastjórn HSS ber ábyrgð á heildaröryggisstefnu stofnunarinnar en Upplýsingaöryggisnefnd undir stjórn forstöðumanns upplýsingamála ber ábyrgð á að framfylgja henni.

Tilvísanir

Hægt er að nálgast frekari upplýsingar um tölvuöryggi á:
http://www.securityfocus.com
http://www.infosyssec.com
Staðallinn ISO/IEC 27001:2005 (Information technology - Security techniques - Information Security Management System – Requirements).
Staðallinn BS-7799

Skilgreiningar

Með orðinu **stjórnandi** er í skjali þessu átt við alla yfirmenn á HSS sem hafa mannaforráð og þurfa þess vegna að sækja um aðgangsheimildir fyrir nýtt starfsfólk
UÖN vísar til nefndar um upplýsingaöryggi HSS

Viðurlög við brotum

Áhersla er lögð á að fylgja settum verklagsreglum og vinnulýsingum. Hvers konar brot á öryggisreglum verða tekin alvarlega. Öll brot verða rannsökuð sérstaklega og geta haft í för með sér refsingar og/eða málaferli.

Afritunarstefna HSS

Afstaða Heilbrigðisstofnunnar Suðurnesja

Öll mikilvæg gögn verður að afrita reglulega. Hægt verður að endurreisa mikilvæg gögn í þá stöðu sem þau voru í við lok síðasta vinnudags, nema hrun eigi sér stað. Eigi hrun sér stað verður að vera hægt að endurbyggja vikugömul gögn.

Réttlæting

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

Tímarammi

Afritunarstefnan er í gildi á öllum tímum.

Hlutverk og ábyrgðir

Notendur: Ábyrgir fyrir að setja mikilvæg gögn á stað þar sem þau verða afrituð.
Tölvunarfræðingur: Ábyrgur fyrir afritunartöku, prófanir á afritum og að uppfæra afritunarskilgreiningar.
Upplýsingaöryggisnefnd: Ábyrgt fyrir að ákveða hvaða gögn skuli vera afrituð.

Framkvæmd

- Einu sinni í viku skal afrita mikilvæg gögn.
- Fjórum sinnum í viku skal gera stigvaxandi afritun (incremental backup) af þeim gögnum breyttust síðan síðasta afritun var gerð.
- Einu sinni í mánuði skal afrita öll gögn á miðlurum.
- Einu sinni á hverjum virkum degi skal skoða skrár (logs) síðustu afritunar og gera viðeigandi ráðstafanir ef þeirra er þörf, s.s. að skipta um spólur, gefa lesréttindi á afritunarnotanda o.þ.h.
- Afritunarskilgreining skal vera endurskoðuð 3 á ári eða eftir þörfum.
- Einu sinni í viku skal setja spólur síðustu viku í eldtraustan peningaskáp.
- Spólur notaðar fyrir vikulegar og daglegar afritanir skal endurnota fjórðu hverja viku.
- Mánaðarlega skal setja spólurnar sem notaðar eru í mánaðarlegri afritun í bankahólf eða álíka öruggan stað.
- Spólur sem notaðar eru fyrir mánaðarafrit má endurnota eftir 12 mánuði. Nema desember spóluna, hana skal ávallt geyma.
- Tvisvar á ári skal prófa að endurbyggja dagleg, vikuleg og mánaðarleg afrit til að kanna heilanleika afritunar.

Frekari upplýsingar

Hægt er að nálgast frekari upplýsingar hjá tölvunarfræðingi.

Breytingar á aðgangsréttindum

Afstaða Heilbrigðisstofnunnar Suðurnesja

Notendur eiga aðeins að fá aðgang að þeim búnaði sem þeir þurfa til að vinna sína vinnu. Þegar aðgangs er ekki lengur þörf skal afturkalla hann. Allar breytingar skal vakta til þess að fylgjast betur með þeim. Þegar talað er um búnað þá er átt við aðgang að tölvubúnaði, hugbúnaði og þeim gögnum sem eru hýst á neti HSS.

Réttlæting

Til að minnka líkurnar á að notendur skemmi óvart gögn sem mikilvæg eru öðrum er mjög mikilvægt að notendur hafi ekki aðgang að kerfum sem þeir þurfa ekki aðgang að. Einnig til að lágmarka líkur á að HSS verði fyrir skaða ef starfsmaður nálgast trúnaðarupplýsingar eða önnur mikilvæg gögn í eigu HSS jafnvel eftir að starfsmaður er hættur að starfa hjá HSS.

Tímarammi

Þessar leiðbeiningar eiga við þegar breytingar á gæðum í kerfinu eiga sér stað.

Hlutverk og ábyrgðir

Stjórnendur: Samþykkir eða hafnar breytingum frá notendum um aðgang að gæðum. Lætur tölvunarfræðing vita um breytingar sem nauðsynlegt er að framkvæma.
Tölvunarfræðingur: Gerir nauðsynlegar breytingar eftir beiðni stjórnenda eða starfsmannastjóra.

Framkvæmd atriðis

- Þegar notendur þurfa aðgang að öðrum kerfum eða gæðum en þeir hafa nú þegar skulu þeir biðja um aðgang í gegnum yfirmann sinn. Þeir skulu rökstyðja hverju hann þarf aðgang að og af hverju.
- Ef stjórnandi samþykkir beiðnina lætur hann tölvunarfræðing framkvæma breytinguna.
- Ef notandi þarf ekki lengur aðgang að gæðum skal tölvunarfræðingur afturkalla réttindi hans að þeim gæðum.

Frekari upplýsingar

Hjá upplýsingaöryggisnefnd eða tölvunarfræðingi.

Reglur um vírusvarnir

Afstaða Heilbrigðisstofnunar Suðurnesja

Heilbrigðisstofnun Suðurnesja er kunnugt um þá hættu sem stafar af vírusum. Öllum brögðum verður að beita til þess að tryggja að vírusar og ormar nái ekki að smita kerfi HSS.

Réttlæting

Vírusasmit og ormasmit geta orsakað gagnatap og –spillingu. Hvorutveggja skaðar hæfni HSS til þess að starfa eðlilega.

Tímarammi

Þessar reglur eiga við á öllum tímum.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Ábyrgur fyrir að útbúa uppsetningarpunkta og viðhalda vírusavörnum fyrir allar tölvur HSS Skal útbúa viðbragðsáætlun gegn vírusasmiti. Ábyrgur fyrir að setja upp vírusvarnaforrit á miðlara. Ábyrgur fyrir setja upp vírusvarnaforrit á vinnustöðvar.

Framkvæmd atriðis

- Tölvunarfræðingur skal útbúa viðbragðsáætlun ef smit verður í samvinnu við upplýsingaöryggisnefnd. Tölvunarfræðingur útbýr uppsetningarpunkt fyrir vírusvarnaforritin og/eða leiðbeiningar um hvernig á að setja þau upp. Sum vírusvarnaforrit hafa sjálfvirka uppsetningu. Ef þannig forrit er valið skal tölvunarfræðingur setja það upp.
- Þegar víruss verður vart skal tölvunarfræðingur fylgja viðbragðsáætluninni.
- Uppsetning vírusvarnaforritsins skal tryggja að tölvan sem það er sett upp á skal vera laus við vírusa. Þetta á við um vírusa sem smitast með tölvupósti, með því að afhlaða af neti eða afrita frá öðrum stöðum s.s. geisladiskum, disklingum eða innra netinu.

Frekari upplýsingar

Hafið samband við tölvunarfræðing.

Reglur um verkflæði fyrir aðkeypta vinnu

Afstaða Heilbrigðisstofnunar Suðurnesja

Heilbrigðisstofnun Suðurnesja veit að oft þarf að úthýsa ýmiskonar upplýsingavinnslu. Sérhæfðir aðilar þurfa oft aðgang að kerfum HSS til uppsetningar á sérhæfðum atriðum. Þetta skapar vissa hættu sem þarf að stjórna.

Réttlæting

Þegar úthýsingu er beitt koma upp ýmsar áhættur. Einstaklingar sem hafa ekki farið í gegnum síunarferli HSS fá aðgang að kerfum stofnunarinnar. Sérstökum aðferðum þarf að beita til þess að tryggja að öryggi kerfisins sé ekki sett í hættu við vinnu þeirra.

Tímarammi

Þetta atriði á við þegar utanaðkomandi aðilar þurfa aðgang að kerfum HSS.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Hann er ábyrgur fyrir að velja hæf fyrirtæki og einstaklinga sem úthýsa þarf til. Þetta gerir hann í samvinnu við þá aðila er verkið varðar.

Framkvæmd atriðis

Þegar einhver sér þörfina fyrir úthýsingu skal sá hinn sami hafa samband við tölvunarfræðing og munu þeir í sameiningu velja hæfan aðila.

Ef aðilarnir þurfa aðgang að tölvukerfinu skal útbúa sérstakan aðgang fyrir þá og fylgjast sérstaklega með honum.

Frekari upplýsingar

Hafið samband við tölvunarfræðing.

Reglur um endurmat

Afstaða Heilbrigðisstofnunar Suðurnesja

Öryggi er samfellt ferli sem þýðir að öll ferli og aðferðir verða að vera í stöðugu endurmati til þess að koma til móts við nýjar áhættur.

Réttlæting

Tryggja verður að öryggi Heilbrigðisstofnunar Suðurnesja verði alltaf gott. Til þess að vera viss um það verður að framkvæma endurmatsaðgerðir reglulega.

Tímarammi

Öryggisstefnuna skal að endurmeta einu sinni á ári. Nota skal janúarmánuð til þessa endurmats.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Ábyrgur fyrir endurmati á öryggisstefnu. Hann skal nýta sér hlutverk annarra aðila, bæði innan stofnunarinnar og utan hennar til þess að gera endurmatið á sem bestan hátt.

Framkvæmd atriðis

- Útbúa skýrslu af öllum frávikum og athyglisverðum atriðum frá síðasta endurmati.
- Gera nýja áhættugreiningu.
- Athuga ef öryggisstefnan stóð sig m.t.t. frábrigðanna og staðla HSS.
- Uppfæra öryggisstefnuna m.t.t. nýrra áhætta og ef hún stóð sig ekki í frábrigðum.
- Rýna uppfærsluna og vera viss um að hún uppfylli kröfur HSS og áhættugreiningarinnar.
- Kynna og framkvæma breytingar.

Frekari upplýsingar

Hafið samband við tölvunarfræðinginn.

Leiðbeiningar um flokkun upplýsinga

Afstaða Heilbrigðisstofnunar Suðurnesja

Starfsfólk Heilbrigðisstofnunar Suðurnesja býr til, viðheldur og vinnur með mikið magn upplýsinga. Þessar upplýsingar eru mjög mismunandi, t.d. varðandi mikilvægi og viðkvæmni þeirra. Þessar leiðbeiningar skilgreina þau öryggisstig sem hægt er að flokka þessar upplýsingar í og gefur jafnframt leiðbeiningar um hvers konar upplýsingar skal setja í hvert stig.

Réttlæting

Viðkvæm gögn verður að vernda. Aðgangi að öllum upplýsingum verður að stjórna til að minnka áhættuna á misnotkun þeirra.

Tímarammi

Þetta atriði á alltaf við.

Hlutverk og ábyrgðir

Upplýsingaöryggisnefnd – Ábyrgt fyrir að búa til og viðhalda þessum leiðbeiningum.

Framkvæmd atriðis

HSS mun hafa 3 stig sem hægt er að flokka upplýsingar í fyrir starfsmenn. Stigin ná frá **Almennu** (minnst viðkvæmt) til **Trúnaðarmál** (mest viðkvæmt).

Almennt: Þetta stig er fyrir upplýsingar sem eru engan veginn viðkvæmar eða mikilvægar HSS Þetta væru t.d. tónlistarskrár, brandarar, myndir og aðrar skrár með takmarkaða notkun.
Starfsfólk á aðeins að hafa les-og-skrif réttindi á það svæði sem skilgreint er fyrir það. Einnig hefur starfsfólk sérstök heimasvæði sem það eitt hefur aðgang að.

Mikilvægt: Þetta stig er fyrir upplýsingar sem hefur einhverja þýðingu fyrir HSS, t.d. almannatengslamál, sniðmát skjala, auglýsingar o.fl. Skrifvakt verður að vera í gangi á þessu svæði.

Trúnaðarmál: Þetta stig er fyrir upplýsingar sem eru HSS og/eða starfsfólki mjög mikilvægar. Dæmi um þess konar upplýsingar væru upplýsingar um sjúklinga. Aðeins útvaldir mega hafa aðgang að þess konar upplýsingum.

Frekari upplýsingar

Hafið samband við tölvunarfræðing.

Reglur um hugbúnað

Afstaða Heilbrigðisstofnunar Suðurnesja

Innan Heilbrigðisstofnunar Suðurnesja er margskonar hugbúnaður notaður í mismunandi tilgangi. Öll notkun hugbúnaðar er háð leyfi og er Heilbrigðisstofnun Suðurnesja umhugað að tryggja að öll leyfi séu lögleg og notkun í hlutfalli við þau.

Réttlæting

Ef leyfislaus hugbúnaður er notaður innan veggja HSS er öryggi og heilindum HSS stefnt í hættu. Þess vegna verður að tryggja rétt leyfi fyrir allan hugbúnað á tölvum HSS.

Tímarammi

Þetta atriði á ávallt við.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Ábyrgur fyrir að viðhalda réttum leyfisupplýsingum á öllum hugbúnað HSS. Ábyrgur fyrir að tölvur séu aldrei með óleyfilegan hugbúnað settan upp.
Notandi – Ábyrgur fyrir að setja aldrei upp hugbúnað án þess að hafa til þess rétt leyfi.

Framkvæmd atriðis

Þegar nýr hugbúnaður er keyptur skal innkaupastjóri halda utan um leyfin sem fylgja hugbúnaðinum.

Frekari upplýsingar

Hafið samband við tölvunarfræðing.

Lykilorð

Afstaða Heilbrigðisstofnunar Suðurnesja

Hver starfsmaður og nemandi skal fá eintækt notendanafn með samsvarandi lykilorði til þess að fá aðgang að tölvukerfi HSS. Lykilorðið býður upp á sannreyningu að aðeins leyfilegir notendur geti nálgast tölvukerfi HSS með þessu eintæka notendanafni.

Réttlæting

Sterkt lykilorðaöryggi tryggir að tölvukerfi séu sem öruggust.

Tímarammi

Þessar reglur um lykilorð eiga við á öllum tímum.

Hlutverk og ábyrgðir

Starfsmaður: Ábyrgur fyrir að tryggja að lykilorð verði ávallt leyndarmál.
Tölvunarfræðingur: Ábyrgur fyrir að útbúa lykilorðastefnu í tölvukerfinu og sannreyna að lykilorð séu nægilega sterk einu sinni á ári með lykilorðabrjótum.

Framkvæmd atriðis

- Tölvunarfræðingur mun útbúa lykilorðastefnu í tölvukerfinu svo lykilorð séu samhæfð þessum reglum.
- Lykilorð skulu vera lágmark 6 stafir.
- Lykilorð mega ekki vera algeng orð eða vægar breytingar á nafni notanda.
- Notendur verða að breyta um lykilorð á a.m.k. einu sinni á ári.
- Notendur hafa aðeins fimm tilraunir til þess að slá inn rétt lykilorð áður en notendanafn læsist.

Frekari upplýsingar

Hægt er að fá frekari upplýsingar hjá tölvunarfræðingi.

Neyðaráætlanir

Afstaða Heilbrigðisstofnunar Suðurnesja

Góð fráviksmeðhöndlun verður að vera til staðar til þess að tryggja lágmarksskemmdir og niðri tíma þegar frávik gerast.

Réttlæting

Frábrigði eru afleiðingar öryggisvandamála. Þessi frábrigði geta eyðilagt innri byggingu HSS og/eða verið mjög dýrar.

Tímarammi

Þessar leiðbeiningar verður að nota við frábrigði.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Ábyrgur fyrir réttum ákvörðunum við frábrigði. Ábyrgur fyrir að endurskoða öryggisstefnuna og athuga hvað er hægt að gera til að koma í veg fyrir frekari frávik.
Starfsmaður – Ábyrgur fyrir að láta tölvunarfræðing vita um frávik.

Framkvæmd atriðis

Dæmi um frávik eru:

- Þú sérð skrýtin feril (process) keyrandi og safnar miklum gjörva tíma.
- Þú hefur uppgötvað að einhver óviðkomandi er að nota kerfið.
- Þú hefur uppgötvað að vírus hefur smitað kerfið.
- Þú hefur ákvarðað að einhver utanaðkomandi er að reyna að brjótast inn í kerfið.
- Þú tekur eftir að hlutir eru horfnir, s.s. lyklaborð, mýs, prentarar o.fl.
- Þú tekur eftir að notandi/starfsmaður er að skemma eignir HSS.
- Þú tekur eftir óvenjulegum breytingum eða villum í uppsetningum miðlara og/eða vinnustöðva.

Við frávik skal strax hafa samband við tölvunarfræðing. Ef frávik gerast utan vinnutíma verður að nota neyðarnúmer tölvunarfræðings.
Ef þú vilt frekar að tilkynningin sé nafnlaus má nota innanhúsnet HSS til þess.
Tölvunarfræðingurinn mun þá meta eðli fráviks, finna ábyrgðaraðila og finna leiðir til þess að leysa frávikið í samvinnu við tengd hlutverk.
Tölvunarfræðingur mun endurmeta öryggisstefnuna og gera viðeigandi breytingar á henni, ef þörf krefur, til þess að koma í veg fyrir svipuð frávik aftur.

Frekari upplýsingar

Frekari upplýsingar er að finna hjá tölvunarfræðingi eða næsta yfirmanni.

Notendaréttindi í tölvukerfinu

Afstaða Heilbrigðisstofnunar Suðurnesja

Notendur eiga aðeins að fá aðgang að þeim gögnum og búnaði sem nauðsynleg eru til þess að þeir geti unnið sitt verk. Þegar þeir þurfa ekki lengur aðgang að þessum gögnum og búnaði skal afturkalla aðgang þeirra.

Réttlæting

Með góðum verklagsreglum næst mun öruggara kerfi.

Tímarammi

Þessar leiðbeiningar eiga við þegar nýr notandi kemur inn í kerfið og þegar notandi fer úr kerfinu.

Hlutverk og ábyrgðir

Starfsmannastjóri – Ábyrgur fyrir að mennta og þjálfa notendur um reglurnar sem eiga við upplýsingaöryggi og notkun tölva. Hann er einnig ábyrgur fyrir að láta þá vita sem þurfa hvenær notandi byrjar við HSS og þegar hann hættir.
Tölvunarfræðingur – Ábyrgur fyrir að setja upp vinnustöðvar notenda miðað við þarfir þeirra og HSS. Býr til/breytir/gerir óvirkan/eyðir notendum í kerfi.
Upplýsingaöryggisnefnd/næsti yfirmaður – Ábyrg fyrir að ákveða að hverju notandi skal hafa réttindi að.
Sjúklingaupplýsingastjóri – Ábyrgur fyrir að gefa starfsmanni þau réttindi sem hann þarfnast í sjúklingaupplýsingakerfi.

Framkvæmd atriðis

Starfsmaður byrjar

- Starfsmannastjóri sjá til þess að notandi lesi notkunarreglur HSS um upplýsingaöryggi og tölvunotkun. Notandi skrifar undir að hann hafi lesið þessar reglur og sé tilbúinn að fylgja þeim.

- Starfsmannastjóri lætur tölvunarfræðing vita að notandinn þurfi aðgang að kerfi og vinnustöð.

- Tölvunarfræðingur láti notanda hafa réttindi skv. ákvörðun næsta yfirmanns.

- Sjúklingaupplýsingastjóri gefur starfsmanni aðgang að sjúklingaupplýsingakerfi samkvæmt óskum næsta yfirmanns.

- Ef notandi er tímabundinn notandi skulu réttindi hans renna út eftir ákveðinn tíma.

Starfsmaður hættir

- Þegar einhver hættir hjá HSS skal starfsmannastjórinn ákveða í samráði við tölvunarfræðing hvaða aðgangi skal afturkalla og/eða eyða.

- Starfsmannastjórinn lætur tölvunarfræðing vita um hvaða réttindi skal afturkalla og hvenær það skal gerast. Þegar starfsmaðurinn er hættur skal eyða notandanum úr kerfinu nema miklar líkur séu á því að hann komi aftur, þá er notandinn gerður óvirkur.

- Þegar starfsmaður hættir skal gera öll lykilorð sem hann gæti vitað óvirk eða eyða þeim.

Frekari upplýsingar

Hægt er að finna frekari upplýsingar hjá starfsmannastjóra eða tölvunarfræðingi.

Notkun vinnustöðva

Afstaða Heilbrigðisstofnunar Suðurnesja

Hver notandi er ábyrgur fyrir þeirri vinnustöð sem hann notar hverju sinni. Með því að fylgja leiðbeiningunum hér fyrir neðan munu notendur fylgja reglum Heilbrigðisstofnun Suðurnesja um notkun vinnustöðva og minnka áhættuna sem steðjar að gögnum þeirra.
Aðgangur að tölvubúnaði, tölvuneti, gögnum og annarri þjónustu sem veitt er hjá HSS er ætlaður til starfa í þágu HSS. Ef einhverjir vilja nota tölvurnar til dægradvalar í einhverju formi eftir vinnutíma, verður það að gerast á þann hátt að það trufli ekki aðra notendur. Þeir verða líka skilyrðislaust að gefa tölvurnar eftir til þeirra sem hyggjast nota þær vegna vinnu.

Réttlæting

Allar vinnustöðvar eru opnar fyrir alls konar áhættu sem getur sett gögn, tæki og vinnu í hættu. Með því að nota vinnustöðvar á ábyrgan hátt er hægt að minnka þessa áhættu.

Tímarammi

Þessar reglur eiga alltaf við.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Ábyrgur fyrir að setja vinnustöðina upp á réttan hátt, skv. stöðlum HSS og að setja upp þau forrit og vélbúnað sem nauðsynlegt er fyrir notandann að sinna vinnu sinni. Ábyrgur fyrir að vakta notkun nets.
Notandi – Ábyrgur fyrir að fylgja þessum reglum.

Framkvæmd atriðis

- Allar innbrotstilraunir inn á kerfin, þar með taldar tilraunir til að komast yfir aðgangsorð og netfang annarra notenda eru stranglega bannaðar.
- HSS er opinber staður og því er skoðun, útprentun og öll miðlun á efni sem særir almennt velsæmi svo sem ósiðlegt efni (klám) bönnuð.
- Óheimilt er að villa á sér heimildir í samskiptum á Netinu, svo sem með því að koma fram undir fölsku nafni í tölvupósti.
- Óheimilt er að setja forrit- eða gögn inn á gagnasvæði eða diska samnýttra vinnustöðva sem notendur hafa aðgang að.
- Óheimilt er að gera breytingar sem hafa áhrif á uppsetningar eða skjáborð samnýttra vinnustöðva, svo sem því að fjarlægja eða breyta kerfisskrám, breyta bakgrunni, táknmyndum eða skjáhvíld sé það hægt.
- Óheimilt er að reyna að komast yfir gögn í eigu annarra notenda nema leyfi þeirra sé fyrir hendi.
- Óheimilt er að reyna að breyta eða hafa áhrif á notkunarmöguleika annarra notenda.
- Öll áreitni á Netinu, sama í hvaða formi hún birtist, er stranglega bönnuð.
- Um allan hugbúnað gilda ákvæði höfundarréttarlaga og því er meginreglan sú að óheimilt er að afrita hugbúnað nema það sé tekið fram í notendaleyfi.
- Notendur tölvukerfisins eiga að stilla útprentunum í hóf, fara sparlega með pappír, taka allar útprentanir og setja gallaðar prentanir í endurvinnslubakka eða

í ruslið. Ef prentverk prentast ekki er óráðlegt að gefa fleiri prentskipanir. Betra er að tilkynna bilunina, koma síðar og taka prentunina.

- Notandinn verður að hafa lykilorð sem samhæfist lykilorðastöðlum HSS.
- Notandinn má aldrei deila lykilorði sínu með neinum. Ekki er ætlast til að hann skrifi lykilorðið niður.
- Aldrei má skilja vinnustöð eftir ólæsta t.d. með skjávaralás.
- Þegar vinnustöð er yfirgefin í meira en 20 mínútur læsist vinnustöðin sjálfkrafa.
- Notkun á vinnustöðinni má bara fela í sér lögmæta notkun sem HSS samþykkir. Þetta felur t.d. ekki í sér klám og annað óæskilegt efni.
- Ekki má notkun kerfisins trufla notandann eða aðra notendur við nauðsynlega vinnu.
- Notkun netsins má ekki brjóta nein lög.
- Notkun netsins má ekki íþyngja því of mikið.
- Ekki má opna viðhengi í tölvupósti nema öruggt sé að það sé laust við vírusa og aðra óværu. Mest hætta stafar af skrám sem enda á EXE eða VBS. Ef notendur eru ekki vissir skulu þeir strax hafa samband við notendaþjónustustjóra.
- Notendur verða að geyma öll gögn á heimadrifinu sínu. Þetta er N:\ drifið. Gögn sem ekki eru geymd þar munu aldrei verða afrituð og eru þar með í áhættu að tapast.
- Gögn sem margir þurfa aðgang að verður að geyma á netinu á stöðum sem miðlarastjóri úthlutar hverjum hópi fyrir sig.

Frekari upplýsingar

Hægt er að nálgast frekari upplýsingar hjá tölvunarfræðingi.

Einkarétturinn

Öll notkun netsins verður skráð niður og reglulega skoðuð. Reglur er varða umgengni um tölvupóst eru á heimasíðu HSS og ber notendum að kynna sér þær. Notendur munu aldrei hafa aðgang að öðrum tölvupósti en sínum eigin.

Reglur um sameiginleg geymslusvæði

Afstaða Heilbrigðisstofnunar Suðurnesja

Notendur tölvukerfis HSS skiptast mjög oft á skrám og upplýsingum í stafrænu formi. Þessar upplýsingar eru mismunandi viðkvæmar og eiga stundum ekki að vera fyrir alla.

Réttlæting

Fólk notast oftast við sameiginleg geymslusvæði til þess að skiptast á gögnum. Til þess að allir geti skipst á öllum tegundum gagna á sem þægilegastan máta verða aðferðir að vera til staðar til þess að hjálpa við það.

Tímarammi

Þetta atriði á ávallt við.

Hlutverk og ábyrgðir

Tölvunarfræðingur – Ábyrgur fyrir að búa til sameignleg geymslusvæði fyrir notendur. Ábyrgur fyrir að setja upp aðgangsstjórnunaraðferðir til þess að stjórna aðgangi í sameiginleg geymslusvæði.

Framkvæmd atriðis

Eitt almennt svæði verður skilgreint fyrir starfsmenn sem vilja skiptast á gögnum. Þetta svæði verður hreinsað mánaðarlega og er aðeins ætlað fyrir gögn sem flytja þarf á milli tölva o.þ.h.
Almenna reglan er sú að þegar hópar þurfa sameiginleg geymslusvæði skal hópstjórinn biðja tölvunarfræðing um að útbúa svæði fyrir hópinn. Hópstjórinn tilgreinir jafnframt hverjir þurfa aðgang að þessu svæði og hver tilgangur þess er. Þegar hópurinn lýkur störfum er hópstjórinn ábyrgur fyrir að láta tölvunarfræðing vita af því að nú megi eyða út svæði hópsins.

Frekari upplýsingar

Hafið samband við tölvunarfræðing.

Meðhöndlun sjúklingaupplýsinga

Afstaða Heilbrigðisstofnunar Suðurnesja

Heilbrigðisstofnun Suðurnesja þekkir þá þörf að allar sjúklingaupplýsingar séu meðhöndlaðar með mestu varkárni og tilliti til sjúklinga. Aðeins til þess bærir aðilar mega hafa aðgang að þessum upplýsingum og réttar aðferðir verða að vera til staðar til þess að tryggja vernd þessara upplýsingar.

Réttlæting

Sjúklingaupplýsingar eru verðmæt gögn. Hægt er að misnota þær á mismunandi máta sem getur skaðað HSS. HSS verður að gera allt sem unnt er til þess að vernda þessar upplýsingar. HSS er einnig gert að virða lög um persónuvernd og meðferð persónuupplýsinga. Þetta er lög frá árinu 2000 nr. 77. Sjá nánar http://www.althingi.is/lagas/nuna/2000077.html.

Tímarammi

Þetta atriði á alltaf við.

Hlutverk og ábyrgðir

Sjúklingaupplýsingastjóri – Ábyrgur fyrir allri meðhöndlun á sjúklingaupplýsingum, hvort sem þær verða til innan HSS eða þeim sem koma utan frá. Hann verður að fylgja verkflæðinu sem lýst er hér að neðan. Ábyrgur fyrir að upplýsingar fari á réttan hátt inn í tölvukerfið.
Upplýsingaöryggisnefnd – Úrskurðarvald um rétta notkun á sjúklingaupplýsingum.
Læknir/ritari – Ábyrgur fyrir að sjúklingaupplýsingar glatist ekki áður en þær eru settar í kerfið og að viðhalda næði þessara upplýsinga.

Framkvæmd atriðis

Þær upplýsingar sem teljast til sjúklingaupplýsinga eru allar persónulegar upplýsingar er varða skjólstæðinga HSS.

Sjúklingaupplýsingastjóri skal tryggja að þessar upplýsingar fái rétta meðferð og geri alla viðeigandi aðila vara við hver sú meðferð er.

Frekari upplýsingar

Hafið sambandi við sjúklingaupplýsingastjóra.

Staðaröryggi

Afstaða Heilbrigðisstofnunar Suðurnesja

Heilbrigðisstofnun Suðurnesja á mikið af tækjum og hlutum, s.s. tölvum, myndvörpum, sjónvörpum o.fl. Skýrar reglur verða að vera til staðar til þess að tryggja rétta meðferð þessara tækja og vernda þau frá stuldi og skemmdum.

Réttlæting

Til að vernda tæki og hluti HSS frá stuldi og skemmdum.

Tímarammi

Þetta atriði á alltaf við.

Hlutverk og ábyrgðir

Umsjónamaður fasteigna- og tækja – Ábyrgur fyrir að útbúa og viðhalda birgðaskrá af vinnustöðvum, fartölvum, miðlurum, skjái, hugbúnaði, jaðartækjum, myndvörpum, sjónvörpum, myndbandstækjum og öllum öðrum tækjum sem hann sér nauðsyn að halda utan um. Hann hefur lyklavöld að öllum læstum hirslum og herbergjum.
Tölvunarfræðingur – Ábyrgur fyrir að útbúa öruggt umhverfi eins og því sem lýst er hér að neðan.
Innkaupastjóri – Ábyrgur fyrir því að láta birgðastjóra vita um hlut sem þarf að setja í birgðaskrá.

Framkvæmd atriðis

- Þær staðaröryggisreglur sem lýst er hér að neðan verður að útfæra.
- Birgðaskráin skal halda utan um nafn hlutar, lýsingu, verðmæti og ábyrgðaraðila.
- Birgðastjóri verður að safna saman öllum þeim hlutum sem hann vill setja í birgðaskrá og tryggja að skráin sé rétt.
- Birgðastjóri skal tryggja að hlutir séu geymdir á öruggan hátt.
- Innkaupastjóri verður að láta birgðastjóra vita um þá hluti sem hann borgar fyrir og gætu þurft að fara í birgðaskrána.
- Geyma verður miðlara í læstum, loftræstum herbergjum.

Frekari upplýsingar

Hafið samband við tölvunarfræðing.

Vakt og endurskoðun

Afstaða Heilbrigðisstofnunar Suðurnesja

HSS skilur að án vaktskráa (auditing logs) eru öryggisráðstafanir ekki eins öflugar og þær gætu verið. Öflug vaktstefna verður að vera til staðar til þess að tryggja gagnsæi? ráðstafana þeirra sem gripið er til. Þessa stefnu verður að endurskoða reglulega til þess að þær séu sem öflugastar. Með öflugri vakt er hægt að nema grunsamlega virkni utan kerfis, sem og innan þess.

Réttlæting

Með því að skoða vaktskrár úr kerfum með það fyrir augum að fylgjast með óæskilegri virkni er hægt að sjá mikið magn upplýsinga. Þessar upplýsingar eru góður mælikvarði á öryggi kerfisins.

Tímarammi

Sú vakt sem útskýrð er hér að neðan skal ávallt vera til staðar. Vaktskrár skal skoða einu sinni í mánuði.

Hlutverk og ábyrgðir

Vaktstjóri – Ábyrgur fyrir að búa til og viðhalda vaktstefnu og áframsenda vaktupplýsingar til viðeigandi hlutverka. Hann skal einnig skoða upplýsingarnar í vaktskránum með tilliti til grunsamlegs athæfis.
Miðlarastjóri – Ábyrgur fyrir að vakta eftirfarandi upplýsingar

- Árangursríkar og –lausar tilraunir til innskráningar á miðlarann.
- Árangursríkar og –lausar tilraunir til notendastjórnunar á miðlaranum.
- Árangurslausar tilraunir til skráasafnaaðgangs.
- Árangursríkar og –lausar tilraunir til stefnubreytinga á miðlara.
- Árangursríkar og –lausar tilraunir til forréttindanotkunar (privilige use).
- Árangursríkar og –lausar tilraunir til þess að komast í gagnaskrár SÖGU.

Tölvunarfræðingur– Ábyrgur fyrir að skoða skrár er varða upplýsingar um misheppnaðar tilraunir til þess að opna tölvupóst annarra. Einnig ábyrgur fyrir að taka úr sambandi “Administrator” aðgang og fylgjast með tilraunum til innskráningar á hann.

Framkvæmd atriðis

Tölvunarfræðingur mun setja grunnreglur vaktar. Allir sem tengjast þessari vaktstefnu verða að fylgja henni skv. vaktstjóra.

Frekari upplýsingar

Hægt er að nálgast frekari upplýsingar hjá vaktstjóra eða í Windows 2000 Security Best Practices á http://www.microsoft.com/technet/security.

Viðauki A

Hlutverk er varða upplýsingaöryggi

Tölvunarfræðingur

- Ber ábyrgð á uppsetningu netkerfisins, s.s. routerum, hubbum, switchum o.fl.
- Sér um að tengingar allra við netið séu fullnægjandi.
- Skjalar uppsetningu netsins.
- Viðheldur skrám yfir hvað er uppsett á hverri vinnustöð s.s. hugbúnaður og ‘hardware’
- Sér um uppsetningu á vinnustöðvunum.
- Ber ábyrgð á að uppfæra hugbúnað og hardware á vinnustöðvum.
- Skjalar uppsetningar vinnustöðvanna.
- Sér um innkaup á vinnustöðvum, skjái og íhlutum.
- Viðheldur skrám yfir hvað er uppsett á hverjum miðlara s.s. hugbúnaður og ‘hardware’
- Sér um uppsetningu á miðlurum.
- Ber ábyrgð á að uppfæra hugbúnað og hardware á miðlurum.
- Skjalar uppsetningar miðlaranna.
- Sér um innkaup á miðlurum, skjái og íhlutum.
- Sér um að setja upp Exchange Server og viðhalda honum.
- Ber ábyrgð á að skjala uppsetningu hans og logga allar aðgerðir á honum.
- Aðstoðar notendur við ýmis vandamál sem upp koma hjá þeim.
- Ber ábyrgð á að skjala aðgerðir sínar.
- Sér um að setja upp vírusvarnir á miðlurum og biðlurum.
- Ber ábyrgð á að uppfæra vírusvarnir.
- Skjalar allar uppfærslur og uppsetningar, kemur á varnarplani.
- Ber ábyrgð á að afrita og prófa gögn af miðlurum.
- Skjalar afritunaráætlun og viðheldur henni.
- Ber ábyrgð á að koma upp neyðaráætlunum, skjala þær og endurskoða.
- Er sá sem fyrst er haft samband við ef vart verður við frábrigði í kerfinu.
- Ber ábyrgð á að setja upp og viðhalda birgðaskrám. Fyrir tölvur, skjái, íhluti, geisladiska og bækur.
- Sér um að setja upp auditing plön, viðhalda þeim og skjala.
- Skoðar audit logga og skjalar viðbrögð við frábrigðum.

- Ber ábyrgð á að framkvæma aðgangsréttindaveitingar og að taka í burtu.
- Býr til notendagrúppur.
- DNS.
- Skjalar aðgangsveitingar-, breytingar- og frátekningar.
- Skjalar grúppur og DNS uppsetningu og breytingar.
- Ber ábyrgð á SQL Server.
- Þ.m.t. uppsetningu og viðhaldi.
- Ber ábyrgð á öllum skjalaþjónum.
- Ber ábyrgð á ytri vefþjóni HSS.
- Ber ábyrgð á vefsíðu HSS og öryggi hennar.
- Ber ábyrgð á innri vefþjóni fyrirtækisins.
- Ber ábyrgð á innri vef fyrirtækisins og öryggi hans.
- Ber ábyrgð á nettengingu fyrirtækisins við umheiminn ásamt skjölun þess.
- Ber ábyrgð á meðferð vinnustöðvar sinnar.
- Verður að fylgja reglum þeim sem settar eru í öryggisstefnu fyrirtækisins.
- Ber ábyrgð á uppsetningu eldveggs og viðhaldi hans.
- Skjalar uppsetningu og heldur til eldveggsstefnu fyrirtækisins.
- Ber ábyrgð á innhringi sambandi starfsmanna.
- Skjalar uppsetningu, hver fær aðgang að því og hvaða skilyrði eru fyrir aðgangi (t.d. personal firewall).
- Ber ábyrgð á virkni prentara og ytri jaðartækja.
- Skjalar viðhald og viðgerðir.

Upplýsingaöryggisnefnd

- Ber ábyrgð á að gera áhættugreiningu og viðhalda henni.
- Skjalar allar uppfærslur á henni.
- Hefur yfirumsjón með aðgerðum þeim er snúa að upplýsingaöryggi.
- Viðheldur öryggisstefnu (security policy) HSS.
- Ber ábyrgð á að öryggisstefna sé til og sé framfylgt.
- Yfirvald fyrirtækisins í upplýsingaöryggismálum.
- Úrskurðarvald í deilumálum.

Sjúklingaupplýsingastjóri (Privacy Manager)

- Ber ábyrgð á að skjala meðferð sjúklingaupplýsinga s.s. sjúkdómasögu o.þ.h.
- Ber ábyrgð á meðferðinni innan HSS.

Starfsmannastjóri (Chief of Staff)

- Ber ábyrgð á aðgangsréttindum starfsfólks. Þ.e. hver fær aðgang og hver ekki.
- Lætur tölvunarfræðing vita af nýjun notendur og hvaða réttindi þeim ber að fá.
- Sér um að setja upp notendanámskeið er snúa að meðferð vinnustöðva og upplýsingaöryggi.
- Setur upp þjálfunaráætlanir og heldur uppi meðvitund starfsmanna um upplýsingaöryggi í fyrirtækinu.
- Lætur tölvunarfræðing vita þegar starfsmenn hætta störfum.

Símkerfisstjóri (Phone System Manager)

- Ber ábyrgð á virkni símkerfis.
- Sér um uppsetningu síma og tengds búnaðar.
- Skjalar viðhald.

Rafkerfisstjóri (Electronics Manager)

- Ber ábyrgð á rafkerfi hússins.
- Sér um viðhald og skjalar það.

Þessum hlutverkum skal úthlutað til einstaklinga sem bera þá jafnframt ábyrgð á þeim sviðum sem undir þau heyra.