Vinnuhandrit Nr. 1

A.
Yfirlýsing um öryggismarkmið Íslenska heilbrigðisnetsins
B.
Leiðbeiningar um lágmarks öryggiskröfur fyrir Íslenska heilbrigðisnetið, byggðar á ÍST ISO/IEC 17799 og ÍST BS 7799-2

Heilbrigðis- og tryggingamálaráðuneytið,
Reykjavík 2002

Yfirlýsing um öryggismarkmið Íslenska heilbrigðisnetsins

Heilbrigðis- og tryggingamálaráðuneytið vill með þessari yfirlýsingu leggja áherslu á mikilvægi upplýsingaöryggis í Íslenska heilbrigðisnetinu. Gögn sem fara um Heilbrigðisnetið eru viðkvæm og verðmæt. Það er því mikilvægt að allir aðilar sem tengjast Heilbrigðisnetinu gæti trúnaðar og tryggi, eftir því sem unnt er, réttleika gagna og að þau séu aðeins tiltæk þeim sem aðgangsrétt hafa. Það er því markmið heilbrigðis- og tryggingamálaráðuneytisins að flutningur viðkvæmra gagna verði tryggður samkvæmt *Leiðbeiningum um lágmarksöryggiskröfur fyrir Íslenska heilbrigðisnetið*.

Ráðuneytið mun stuðla að því að veitt verði nægjanlegum fjármunum og mannafla til þess að tryggja rekstur Heilbrigðisnetsins og öryggi sjúkragagna á viðeigandi hátt að teknu tilliti til þeirrar áhættu sem til staðar er hverju sinni.

Öryggisstefnan byggist m.a. á ákvæðum í lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga og reglugerð settri skv. ofangreindum lögum. Öll starfræksla Íslenska heilbrigðisnetsins skal fara að lögum og reglum sem um starfsemina gilda.

Þeir aðilar sem tengjast vilja Heilbrigðisnetinu skulu hafa eigin öryggisstefnu sem samræmist öryggismarkmiði Heilbrigðisnetsins. Þá skulu aðilar sem tengjast Heilbrigðisnetinu hafa öryggishandbók og skulu þeir og gögn sem frá þeim fara um Heilbrigðisnetið uppfylla lágmarksöryggiskröfur netsins sem byggja á ÍST ISO/IEC 17799:2000 og ÍST BS 7799-2:1999.

Aðeins þeir aðilar sem hafa fengið staðfestingu heilbrigðis- og tryggingamálaráðuneytisins um að uppfylla lágmarksöryggiskröfur Heilbrigðisnetsins fá aðgang að því og geta sent heilsufarsgögn um netið. Sérhver þessara aðila skal tryggja að heilsufarsgögn séu aðeins send til þeirra sem rétt hafa til móttöku gagnanna.

Heilbrigðis- og tryggingamálaráðuneytið ber ábyrgð á þessari yfirlýsingu. Ráðuneytið skipar sérstakan umsjónarmann með starfrækslu Heilbrigðisnetsins og er hann jafnframt öryggisstjóri þess. Skal hann bera ábyrgð á að öryggismarkmiðið sé endurskoðað árlega, oftar ef tilefni er til t.d. vegna viðbragða við frávikum, nýjum veikleikum og mikilvægum breytingum á skipulagi eða tæknilegum innviðum. Yfirlýsing þessi um öryggismarkmið Heilbrigðisnetsins skal vera aðgengileg öllum sem aðgang hafa að því.

Leiðbeiningar um lágmarks öryggiskröfur fyrir Íslenska heilbrigðisnetið, byggðar á ÍST ISO/IEC 17799 og ÍST BS 7799-2

1. Umfang

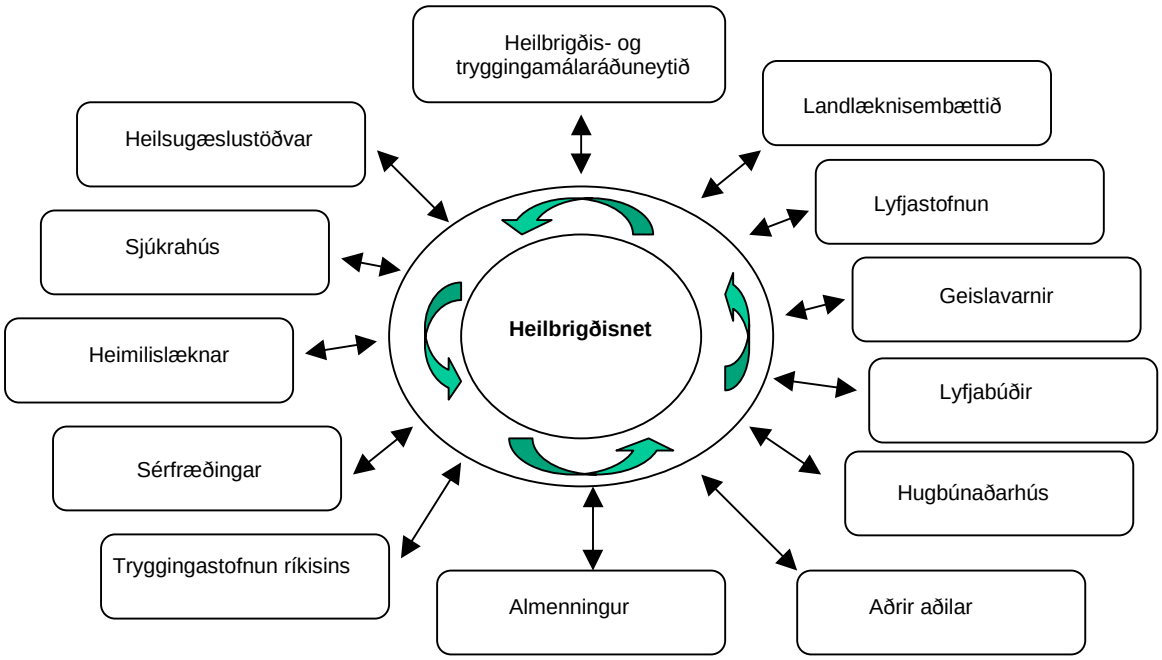
Í þessum leiðbeiningum eru tilgreindar kröfur sem gerðar eru til þeirra aðila sem hafa, eða óska eftir að fá, aðgang að Íslenska heilbrigðisnetinu. Kröfurnar eru byggðar á öryggisstaðlinum ÍST ISO/IEC 17799:2000[1] og ÍST BS 7799-2:1999[1] og gilda um að taka upp, innleiða og skjalfesta stjórnkerfi upplýsingaöryggis[1].

2. Hugtök og skilgreiningar

Íslenska heilbrigðisnetið

Íslenska heilbrigðisnetið skal vera öruggur farvegur rafrænna samskipta milli aðila innan heilbrigðisþjónustu. Það er samskipta- og upplýsingatæki heilbrigðiskerfisins og um það fara mjög viðkvæmar persónuupplýsingar. Heilbrigðisnetið er net sem notar almennar flutningsleiðir. Allir aðilar sem tengjast netinu eru hluti af því og bera jafna ábyrgð. Heilbrigðisnetið samanstendur af upplýsingakerfum einstakra aðila sem tengjast því og þeim fjarskiptabúnaði sem tengir þá saman auk samskipta- og öryggisreglna.

(Orðskýringar eru í viðauka A.)



[1] Í orðskýringum í viðauka A er að finna nánari skýringu á merktum orðum eða hugtökum.

3. Kröfur um stjórnkerfi upplýsingaöryggis[1] fyrir Íslenska heilbrigðisnetið

3.1. Almennt

Aðilar sem tengjast Íslenska heilbrigðisnetinu skulu koma á og viðhalda skjalfestu stjórnkerfi upplýsingaöryggis[1]. Kerfið skal taka mið af eignum[1] sem ætlunin er að vernda, aðferðum aðila við áhættustjórnun[1], stýringarmarkmiðum[1] og ráðstöfunum[1] og öryggisstigi sem krafist er.

4. Nánar tilgreindar ráðstafanir

4.1. Öryggisstefna[1]

Markmið: Að stjórnendur hafi forystu um og styðji við öryggi upplýsinga.

- Stjórnendur skulu samþykkja öryggisstefnu[1], birta hana og miðla upplýsingum um hana til allra starfsmanna eftir því sem við á.
- Öryggisstefnuna[1] skal rýna og endurskoða reglulega og þegar áhrifavaldandi breytingar eiga sér stað, til að tryggja að hún eigi ávallt við.

4.2. Skipulag öryggismála

4.2.1. Innviðir upplýsingaöryggis[1]

Markmið: Að stjórna upplýsingaöryggi[1] innan Íslenska heilbrigðisnetsins.

- Koma skal á samráðsvettvangi stjórnenda um öryggismál.
- Setja skal skýrar reglur um ábyrgð og varnir einstakra verðmæta.
- Leita skal til aðila með sérfræðiþekkingu á öryggismálum eftir því sem við á.
- Hafa skal virkt samstarf við aðila eins og lögreglu, Persónuvernd, upplýsingaþjónustur og fjarskiptafyrirtæki.
- Óháður aðili skal endurskoða framkvæmd öryggisstefnunnar.

4.2.2. Öryggismál vegna aðgangs utanaðkomandi aðila

Markmið: Að viðhalda öryggi hjá aðilum Íslenska heilbrigðisnetsins varðandi upplýsingavinnslubúnað þess og upplýsingaeignir[1] sem utanaðkomandi aðilar hafa aðgang að.

- Meta skal áhættu[1] sem því fylgir að þriðji aðili hafi aðgang að upplýsingakerfum aðila.

- Gera skal formlegan samning um aðgang þriðja aðila þar sem fram koma allar nauðsynlegar upplýsingar varðandi öryggiskröfur.

4.2.3. Útvistun

Markmið: Að viðhalda öryggi upplýsinga þegar ábyrgð á upplýsingavinnslu hefur verið vistuð hjá öðru fyrirtæki, sbr. 13 gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, reglur um öryggi persónuupplýsinga nr. 299/2001 og lög um réttindi sjúklinga nr. 74/1997.

- Gera skal formlegan samning um útvistun upplýsinga og upplýsingakerfa þar sem fram kemur hvaða öryggisráðstafanir[1] eru nauðsynlegar til þess að tryggja öryggi gagnanna.

4.3 Flokkun eigna[1] og stýring þeirra

4.3.1. Ábyrgð á eignum[1]

Markmið: Að halda uppi viðeigandi vernd fyrir eignir[1] aðila.

- Halda skal skrá yfir öll mikilvæg verðmæti.

4.3.2. Flokkun upplýsinga

Markmið: Að tryggja að upplýsingaeignir[1] njóti viðeigandi verndar.

- Skilgreina skal kerfi fyrir flokkun gagna ásamt viðeigandi meðhöndlun og öryggisráðstöfunum[1].

- Skilgreina skal verkferla sem tryggja að verðmæti verði flokkuð rétt og fái viðeigandi merkingu, m.a. með tilliti til gr. 8 og 9 í lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

4.4. Starfsmenn og öryggi

4.4.1. Öryggi í starfslýsingum og ráðningum

Markmið: Að draga úr hættu á mannlegum mistökum, þjófnaði, svikum eða misnotkun búnaðar.

- Starfslýsingar skulu innihalda lýsingu á ábyrgð og hlutverki gagnvart öryggi.

- Við ráðningu starfsmanna skal fara eftir reglum um sannprófun[1] upplýsinga.

- Starfsmenn skulu undirrita trúnaðaryfirlýsingu.

4.4.2. Þjálfun notenda

Markmið: Að tryggja að notendur viti af ógnunum gegn öryggi upplýsinga og áhyggjum af þeim og að þeir séu undir það búnir að fylgja öryggisstefnu[1] Íslenska heilbrigðisnetsins í daglegu starfi sínu.

- Allir starfsmenn aðila sem tengjast Heilbrigðisnetinu og einnig utanaðkomandi notendur, þar sem það á við, skulu fá viðeigandi þjálfun og reglubundna endurnýjaða fræðslu um stefnu Heilbrigðisnetsins og verklagsreglur.

4.4.3. Viðbrögð við villum og öryggisfrávikum[1]

Markmið: Að lágmarka tjón af villum og öryggisfrávikum[1], vakta slík frávik og læra af þeim.

- Öll öryggisbrot skal tilkynna til viðeigandi aðila við fyrsta tækifæri eftir að þau uppgötvast.

- Allir notendur upplýsingakerfa verða að skrá og tilkynna öryggisfrávik[1] sem þeir verða varir við eða telja hugsanleg.

- Skilgreina skal agaviðurlög við öryggisbrotum.

4.5. Raunlægt öryggi[1] og umhverfisöryggi

4.5.1. Örugg svæði

Markmið: Að koma í veg fyrir óheimilan aðgang, tjón eða truflanir á starfssvæði aðila og upplýsingum hans.

- Aðili skal afmarka örugg svæði þar sem búnaður til vinnslu upplýsinga er komið fyrir.

- Örugg svæði skal vernda með viðeigandi stýringu á aðgengi til þess að tryggja að aðeins aðilum með heimild sé hleypt inn.

- Setja skal upp örugg svæði til þess að vernda skrifstofur, herbergi og búnað þar sem gerðar eru sérstakar öryggiskröfur.

- Nota skal viðbótarráðstafanir og leiðbeiningar um vinnu á öruggum svæðum til þess að auka við öryggið sem fæst með þeim raunlægu ráðstöfunum[1] sem gerðar eru til verndar öruggum svæðum.

4.5.2. Öryggi tækjabúnaðar

Markmið: Að koma í veg fyrir að eignir[1] glatist eða skemmist eða þeim sé stefnt í hættu og koma í veg fyrir röskun á rekstrinum.

- Tækjabúnað skal staðsetja eða vernda þannig að dregið sé úr áhættu[1] af ógnunum[1] og háska í umhverfinu og tækifærum til óheimils aðgangs.

- Fjarskiptalagnir sem flytja gögn eða styðja upplýsingaþjónustu Heilbrigðisnetsins skal verja fyrir hlerun og skemmdum.

- Eyða skal upplýsingum af tækjabúnaði áður en honum er fargað eða hann er endurnýttur.

4.5.3. Almennar ráðstafanir

Markmið: Að koma í veg fyrir að upplýsingum og búnaði til vinnslu þeirra sé stofnað í hættu eða stolið.

- Aðili skal koma á og innleiða verklagsreglur um að ekkert sé skilið eftir á glámbekk, hvorki hlutir á borðum né upplýsingar á skjám, til þess að draga úr hættu á óheimilum aðgangi og að upplýsingar glatist eða spillist.

- Tækjabúnað, upplýsingar eða hugbúnað í eigu eða umsjá aðila má ekki fjarlægja án heimildar.

4.6. Stjórnun á samskiptum og rekstri

4.6.1. Verklagsreglur um rekstur og ábyrgð á rekstri

Markmið: Að tryggja réttan og öruggan rekstur búnaðar til upplýsingavinnslu.

- Þær verklagsreglur um rekstur, sem tilgreindar eru í upplýsinga-öryggisstefnu[1] (sbr. 4.1), skulu vera skjalfestar og þeim skal haldið við.

- Breytingum á búnaði og kerfum til upplýsingavinnslu skal vera stýrt.

- Ákveða skal ábyrgð og setja verklagsreglur um meðferð frávika til þess að tryggja skjót, skilvirk og skipuleg viðbrögð.

- Aðskilja skal skylduverk og ábyrgðarsvið til þess að draga úr tækifærum til óheimilla breytinga eða misnotkunar á upplýsingum eða þjónustu.

- Búnaði fyrir þróun og prófun skal halda aðskildum frá rekstrarbúnaði.

4.6.2. Skipulagning og samþykki kerfa

Markmið: Að lágmarka áhættu[1] á bilunum í kerfum.

- Ákvarða skal viðmið um samþykki á nýjum upplýsingakerfum, uppfærslum og nýjum útgáfum og gera viðeigandi prófanir á kerfunum áður en samþykki er veitt.

4.6.3. Vernd gegn spillihugbúnaði[1]

Markmið: Að vernda réttleika hugbúnaðar og upplýsinga.

- Setja skal upp búnað til að greina, hindra virkni og eyða spillihugbúnaði[1], svo og viðeigandi verklagsreglur til þess að efla öryggisvitund notenda.

- Skilgreina skal lágmarkskröfur til virkni búnaðar sem notaður er til þess að verjast spillihugbúnaði[1].

4.6.4. Dagleg umsjón

Markmið: Að sjá til þess að upplýsingavinnslu- og samskiptaþjónusta sé ávallt tiltæk og starfi rétt.

- Reglulega skal afrita nauðsynlegar upplýsingar og hugbúnað.

- Starfsfólk, sem annast rekstur kerfa tengdum Heilbrigðisnetinu, skal halda dagbók um störf sín.

- Skýra skal frá villum og gera úrbætur.

4.6.5. Netstjórn

Markmið: Að tryggja verndun upplýsinga í netum og innviða sem þau styðjast við.

- Innleiða skal ráðstafanir til þess að tryggja öryggi í netum.

4.6.6. Meðhöndlun og öryggi miðla

Markmið: Að koma í veg fyrir tjón á eignum og truflun á starfssemi.

- Umsjón með færanlegum gagnamiðlum, svo sem diskum, segulböndum, geisladiskum og prentuðum skýrslum, skal lúta eftirliti.

- Farga skal miðlum með tryggum og öruggum hætti þegar þeirra er ekki lengur þörf.

- Setja skal verklagsreglur um meðhöndlun og geymslu upplýsinga til að vernda þær fyrir óheimilli uppljóstrun eða misnotkun.

4.6.7. Skipti á upplýsingum og hugbúnaði

Markmið: Að koma í veg fyrir að upplýsingar sem berast milli aðila glatist, breytist eða séu misnotaðar.

- Gera skal formlega samninga við heilbrigðisyfirvöld um skipti, rafræn eða önnur, á upplýsingum og hugbúnaði meðal aðila sem tengjast Heilbrigðisnetinu.

- Vernda skal gögn og miðla, sem eru í flutningi, fyrir óheimilum aðgangi, misnotkun eða spillingu.

- Vernda skal rafræn samskipti/viðskipti fyrir sviksamlegu athæfi, samningsdeilum og uppljóstrun eða breytingu á upplýsingum.

- Móta skal stefnu um notkun tölvupósts og koma á eftirliti til þess að draga úr öryggisáhættu vegna hans.

- Upplýsingar, sem sendar eru til aðila, sem ekki eru hluti af Heilbrigðisnetinu, skulu fara í gegnum formlegt heimildaferli áður en þær eru sendar.

- Koma skal á verklagsreglum og ráðstöfunum til þess að vernda upplýsingaskipti um talsíma, fax og fjarfundabúnað.

4.7. Aðgangsstýring

4.7.1. Rekstrarkröfur um aðgangsstýringu

Markmið: Að stýra aðgangi að upplýsingum.

- Reglur um aðgang skulu fylgja tilmælum landlæknis um aðgang að sjúkragögnum í tölvukerfum og laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.

- Rekstrarlegar kröfur um aðgangsstýringu ber að skilgreina og skjalfesta, og takmarka skal aðgang við skilgreinda stefnu um aðgangsstýringu.

4.7.2. Stýring á aðgangi notenda

Markmið: Að koma í veg fyrir óheimilaðan aðgang að upplýsingakerfum sem notuð eru til samskipta á Heilbrigðisnetinu.

- Í gildi skulu vera formlegar verklagsreglur um skráningu og afskráningu notenda vegna aðgangs að öllum upplýsingakerfum og þjónustu ætluðum mörgum notendum.
- Úthlutun og notkun sérréttinda[1] skal háð takmörkunum og stýringu.
- Úthlutun aðgangsorða skal stýra með formlegu ferli.
- Aðgangsréttindi notenda skal rýna samkvæmt formlegu ferli með reglulegu millibili.

4.7.3. Ábyrgð notenda

Markmið: Að koma í veg fyrir óheimilan notendaaðgang.

- Gera skal kröfu til notenda um að þeir fylgi góðum öryggisvenjum við val og notkun aðgangsorða.
- Gera skal kröfu til notenda um að þeir tryggi að allur eftirlitslaus tækjabúnaður njóti viðeigandi verndar.

4.7.4. Stýring á netaðgangi

Markmið: Að vernda netþjónustu.

- Notendum skal aðeins veita beinan aðgang að þeirri þjónustu sem þeir hafa sérstaklega fengið heimild til.
- Hafa skal eftirlit með leiðinni frá útstöð notanda til tölvuþjónustu.
- Fjartengdir notendur skulu sæta sannvottun[1] áður en þeir fá aðgang.
- Tengingar við ytri tölvukerfi skulu háðar sannvottun[1].
- Hafa skal eftirlit með tengingum um ytri netbúnað og koma upp viðeigandi vörnum til að verjast óleyfilegum aðgangi sem notfærir sér veikleika í búnaðinum (eldveggjum[1] og beinum[1]).
- Gera skal ráðstafanir í netum til þess að skilja að upplýsingaþjónustuhópa, notendahópa og upplýsingakerfi.

- Tengigeta notenda í sameiginlegum netum skal háð takmörkunum samkvæmt stefnu um aðgangsstýringu.

- Skýr lýsing skal vera fyrir hendi á öryggisþáttum allrar netþjónustu sem aðilinn notar.

4.7.5. Stýring á aðgangi að stýrikerfi

Markmið: Að koma í veg fyrir óheimilan aðgang að tölvum.

- Nota skal sjálfvirk kennsl á útstöð til þess að sannvotta[1] tengingar, þegar eingöngu skal vera hægt að hefja vinnslu frá tilteknum stað eða útstöð.

- Aðgangur að upplýsingaþjónustu[1] skal vera um öruggt innskráningar-ferli.

- Allir notendur skulu hafa einkvæmt[1] auðkenni (notendakenni) til eigin nota eingöngu þannig að síðar sé hægt að rekja aðgerðir til þess notanda sem er ábyrgur fyrir þeim.

- Í gildi skal vera aðgangsorðakerfi með skilvirkum, gagnvirkum búnaði sem tryggir góð aðgangsorð.

- Óvirkar útstöðvar á áhættusvæðum, eða sem þjóna áhættukerfum, skulu slökkva á sér eftir skilgreindan tíma aðgerðarleysis til þess að koma í veg fyrir óviðkomandi aðgang.

- Beita skal takmörkunum á tengitíma til þess að veita aukið öryggi í notendahugbúnaði þar sem áhætta er mikil.

4.7.6. Stýring aðgangs að notendahugbúnaði

Markmið: Að koma í veg fyrir óheimilan aðgang að upplýsingum sem geymdar eru í upplýsingakerfum.

- Aðgengi að upplýsingum skal takmarka samkvæmt stefnu um aðgangsstýringu.

- Viðkvæm kerfi skulu höfð í aðskildu (þ.e. einangruðu) vinnslu-umhverfi.

4.7.7. Vöktun á kerfisaðgangi og notkun

Markmið: Að greina óheimilar aðgerðir.

- Úttektardagbækur[1], þar sem skráðar eru undantekningar og aðrir atburðir er tengjast öryggismálum, skulu haldnar og geymdar í

tilgreindan tíma til að nota við síðari rannsóknir og vöktun á aðgangsstýringu.

- Setja skal verklagsreglur um vöktun búnaðar til upplýsingavinnslu og rýna niðurstöður vöktunarinnar með kerfisbundnum hætti.

- Tölvuklukkur skal samstilla til þess að fá nákvæmar skráningar.

4.7.8. Fartölvur, fjarvinna[1] og fjarþjónusta[1]

Markmið: Að tryggja öryggi upplýsinga þegar notaðar eru fartölvur, aðstaða til fjarvinnu[1] og fjarþjónusta[1]

- Formleg stefna skal vera í gildi og gera skal viðeigandi ráðstafanir varðandi hættu sem tengist vinnu með fartölvubúnaði, einkum í óvernduðu umhverfi.

- Móta skal stefnu og verklagsreglur um að heimila og stýra fjarvinnu[1].

- Öryggisstig á fjarvinnustað skal vera í samræmi við öryggisflokkun þeirra upplýsinga sem unnið er með í fjarvinnu[1].

- Reglur um fjarþjónustu[1] skulu fylgja leiðbeiningum í viðauka B í tilmælum landlæknis vegna öryggis sjúkragagna í tölvum.

4.8. Þróun og viðhald kerfa

4.8.1. Öryggiskröfur vegna kerfa

Markmið: Að tryggja að öryggi sé innfellt í upplýsingakerfi.

- Tryggt skal að öryggi sé innfellt í öll upplýsingakerfi Íslenska heilbrigðisnetsins í samræmi við öryggismarkmið þess.

- Skilgreina skal og skjalfesta öryggiskröfur áður en hugbúnaðargerð hefst.

- Gera skal áhættumat[1] og beita áhættustjórnun[1] til þess að ákvarða öryggiskröfur og velja aðgerðir skv. ÍST ISO/IEC 17799:2000[1] og ÍST BS 7799-2:1999[1] til þess að stjórna áhættunni.

4.8.2. Öryggi í hugbúnaðarkerfum

Markmið: Að koma í veg fyrir að notendagögn í hugbúnaðarkerfum glatist, breytist eða séu misnotuð.

- Sannprófa[1] skal inntaksgögn sem notuð eru á Heilbrigðisnetinu til þess að tryggja að þau séu rétt og viðeigandi.

- Sannvottun[1] skeyta skal notuð á Heilbrigðisnetinu þar sem gerð er krafa um að vernda réttleika[1] innihalds.

4.8.3. Ráðstafanir með dulritun

Markmið: Að viðhalda leynd[1], áreiðanleika[1] og réttleika[1] upplýsinga.

- Móta skal og framfylgja stefnu um notkun dulritunar til þess að vernda upplýsingar.

- Beita skal dulritun til þess að viðhalda leynd viðkvæmra eða mikilvægra upplýsinga.

- Beita skal rafrænum undirskriftum[1] til þess að viðhalda áreiðanleika[1] og réttleika[1] rafrænna upplýsinga.

- Nota skal umsjónarkerfi með lyklum sem byggist á umsömdum stöðlum, verklagsreglum og aðferðum til þess að styðja við notkun dulmálstækni.

4.8.4. Öryggi kerfisskráa

Markmið: Að tryggja að öryggis sé gætt í verkefnum í upplýsingatækni og starfsemi til stuðnings þeim.

- Innleiðingu hugbúnaðar skal stýra í kerfum sem eru notuð í samskiptum um Heilbrigðisnetið.

- Prófunargögn skulu njóta verndar og vera undir eftirliti.

- Prófunargögn mega aldrei innihalda persónugreinanleg gögn.

- Aðgangur að frumforritasöfnum[1] skal vera undir strangri stýringu.

4.8.5. Öryggi í þróunar- og stuðningsferlum

Markmið: Að viðhalda öryggi hugbúnaðarkerfa og upplýsinga.

- Innleiðing breytinga skal fylgja ströngum, formlegum verklagsreglum um stýringu á breytingum til þess að koma í veg fyrir spillingu upplýsingakerfa.

- Hugbúnaðarkerfi skal rýna og prófa þegar breytingar eru gerðar á stýrikerfi.

- Forðast skal að breyta hugbúnaðarpökkum, en nauðsynlegar breytingar skulu vera undir ströngu eftirliti.

- Stýra skal kaupum, notkun og breytingum á hugbúnaði og hafa eftirlit með honum til að verjast hugsanlegum laumurásum[1] og trójuhestum[1].

- Beita skal ráðstöfunum til þess að tryggja öryggi aðkeyptrar hugbúnaðarþróunar.

4.9. Stjórnun á samfelldum rekstri[1]

4.9.1. Þættir stjórnunar á samfelldum rekstri[1]

Markmið: Að vinna gegn röskun á rekstri og vernda mikilvæg rekstrarferli fyrir áhrifum af meiri háttar bilunum eða stóráföllum.

- Til að tryggja samfelldan og órofinn rekstur Heilbrigðisnetsins er mikilvægt að draga sem mest úr hættu á hvers konar áföllum.

- Til þess að verjast áföllum og lágmarka skaða sem hlýst af þeim skal grípa til ráðstafana varðandi eftirtalin atriði:
  a) Starfsreglur og umgengni hjá aðilum sem eru tengdir Heilbrigðisnetinu.
  b) Tryggingamál
  c) Öryggisafritun og varðveisla þeirra
  d) Áætlanir um samfelldan rekstur, greining á áföllum og viðbrögð

- Koma skal á verkferlum sem miða að því að tryggja samfelldan rekstur.

- Móta skal langtímaáætlun, byggða á viðeigandi áhættumati[1], þar sem lýst er heildaráformum aðila sem tengjast Heilbrigðisnetinu varðandi samfelldan rekstur.

- Semja skal áætlanir til þess að halda rekstri gangandi eða koma honum í gang aftur án langrar tafar eftir röskun á mikilvægum rekstrarferlum.

- Samræma skal aðgerðir til þess að tryggja samfelldan rekstur.

- Áætlanir til þess að tryggja samfelldan rekstur skal prófa, viðhalda og endurmeta með reglubundnum hætti.

4.10. Fylgni

4.10.1. Fylgni við réttarfarsleg ákvæði

Markmið: Að komast hjá brotum gegn refsirétti og einkamálarétti, lögbundnum, reglugerðarbundnum eða samningsbundnum skyldum og hvers kyns öryggiskröfum.

- Lög sem varða starfsemi Íslenska heilbrigðisnetsins eru m.a.:
  - Lög um heilbrigðisþjónustu 1990 nr. 97 28. september
  - Lög um læknaráð 1942 nr. 14 15. maí
  - Lög um réttindi sjúklinga 1997 nr. 74 28. maí
  - Lög um gagnagrunn á heilbrigðissviði 1998 nr. 139 22. desember
  - Lög um lífsýnasöfn 2000 nr. 110 25. maí
  - Lög um persónuvernd og meðferð persónuupplýsinga 2000 nr. 77 23. maí
  - Lög um slysavarnaráð 1994 nr. 33 25. apríl
  - Lög um málefni aldraðra 1999 nr. 125 31. desember
  - Lyfjalög 1994 nr. 93 20. maí
  - Upplýsingalög 1996 nr. 50 24. maí
  - Lyfsölulög 1963 nr. 30 29. apríl
  - Lög um aðbúnað, hollustuhætti og öryggi á vinnustöðum 1980 nr. 46 28. maí
  - Lög um almannavarnir 1962 nr. 94 29. desember

- Lög um heilbrigðisstéttir:
  - Lög um starfsheiti og starfsréttindi heilbrigðisstétta 1985 nr. 24 28. maí
  - Læknalög 1988 nr. 53 19. maí
  - Hjúkrunarlög 1974 nr. 8 13. mars
  - Lög um sjúkraþjálfun 1976 nr. 58 31. maí
  - Lög um iðjuþjálfun 1977 nr. 75 31. desember
  - Lög um sjúkraliða 1984 nr. 58 28. maí
  - Lög um lyfjafræðinga 1978 nr. 35 11. maí
  - Lög um tannlækningar 1985 nr. 38 12. júní
  - Lög um starfsréttindi tannsmiða 2000 nr. 109 25. maí
  - Lög um sjóntækjafræðinga 1984 nr. 17 24. apríl

- Innleiða skal viðeigandi verklagsreglur til þess að tryggja að fylgt sé lagalegum skorðum við notkun efnis sem kann að vera háð hugverkarétti og við notkun hugbúnaðar sem bundinn er eignarétti.

- Mikilvægar skrár Íslenska heilbrigðisnetsins skal vernda fyrir glötun, eyðileggingu og fölsun.

- Beita skal ráðstöfunum[1] til þess að vernda persónuupplýsingar sem fara um Heilbrigðisnetið í samræmi við gildandi lög.

- Notkun aðila Heilbrigðisnetsins á búnaði til upplýsingavinnslu skal háð heimild stjórnenda og beita skal ráðstöfunum til þess að koma í veg fyrir misnotkun hans.

- Ráðstafanir[1] skulu vera fyrir hendi til þess að tryggja að farið sé eftir samningum, lögum, reglugerðum eða öðrum fyrirmælum við stýringu á aðgangi að dulritun og notkun hennar.

- Þegar aðgerðir sem gripið er til gegn einstaklingi eða lögaðilum eru lagalegs eðlis, hvort heldur samkvæmt refsirétti eða einkamálarétti, skulu sönnunargögn sem lögð eru fram uppfylla lagaákvæði um sönnunargögn eða reglur þess dómstóls þar sem mál verður rekið. Í því skal m.a. felast að hlítt sé hvers kyns birtum stöðlum eða starfsvenjum um framlagningu lögmætra sönnunargagna.

4.10.2. Rýni á öryggisstefnu[1] og tæknilegu samræmi[1]

Markmið: Að tryggja að kerfi fylgi öryggisstefnu[1] Heilbrigðisnetsins og öryggisstöðlum.

- Stjórnendur skulu tryggja að öllum verklagsreglum um öryggi á þeirra ábyrgðarsviði sé framfylgt með réttum hætti og öll starfssvið aðila sem tengjast Heilbrigðisnetinu skulu háð reglubundinni rýni til þess að tryggja að öryggisstefnu[1] og öryggisstöðlum sé fylgt.

- Kanna skal starfsrækslu Íslenska heilbrigðisnetsins með reglubundnum hætti til að ganga úr skugga um hvort upplýsingakerfi fylgi stöðlum um innleiðingu öryggis.

4.10.3. Atriði sem huga ber að við úttekt kerfa

Markmið: Að hámarka skilvirkni úttektarferlisins og lágmarka truflun sem verður á og leiðir af því.

- Úttektir á kerfum í rekstri skal skipuleggja og ná samkomulagi um þær til þess að halda hættunni á truflunum á rekstrarferlum í lágmarki.

- Aðgengi að verkfærum til úttektar kerfa skal vernda til þess að koma í veg fyrir að þau séu misnotuð á einhvern hátt eða þeim sé stofnað í hættu.

Viðauki A Orðskýringar

áhætta: möguleikinn að tiltekin ógnun[1] mun notfæra sér veikleika[1] eignar eða hóps eigna til að valda tapi eða tjóna á eignum.

áhættumat: ferlið við að auðkenna öryggisáhættur sem steðja að upplýsingum og upplýsingavinnslu, ákveða umfang þeirra og áhrif og auðkenna svæði sem þarf að verja.

áhættustjórnun: heildarferlið við að auðkenna, stjórna og útrýma eða lágmarka óvissa atburði sem geta haft áhrif á öryggi upplýsingakerfa.

áreiðanleiki: eiginleikinn sem felur í sér mótsagnalausa ætlaða hegðun og niðurstöður.

beinir: (e. router) búnaður sem notaður er til að stjórna netsamskiptum, þ.e. beina þeim rétta leið.

eign: eitthvað sem hefur gildi fyrir aðila.

einkvæmt notendakenni: notendakenni (notendanafn) sem enginn annar hefur eða notar.

eldveggur: (e. firewall, einnig kallað netvari, netveggur, netvörn) búnaður sem settur er upp til að verja innra net aðila fyrir óheimilum aðgangi frá ytra neti (t.d. Interneti).

fjarvinna: vinna sem fer fram utan aðstöðu aðila, þarf ekki að vera um fjartengingu.

fjarþjónusta: þjónusta sem þriðji aðili veitir í gegnum fjartengingu.

frumforritasafn: skráarsafn, eða söfn, sem inniheldur frumkóða forrita.

ÍST ISO/IEC 17799:2000 og ÍST BS 7799-2:1999: Íslenskur staðall í tveimur hlutum er lýtur að öryggi upplýsinga og upplýsingakerfa. Fyrri hlutinn er þýðing á alþjóðlega staðlinum ISO/IEC 17799:2000 sem upphaflega var fyrri hluti breska staðalsins BS 7799 (BS 7799-1:1998). Seinni hlutinn er þýðing á seinni hluta breska staðalsins BS 7799 (BS 7799-2:1999).

laumurásir: dulinn kóði í forritum sem er notaður til að afhjúpa upplýsingar með beinum eða óbeinum hætti.

leynd: trygging þess að upplýsingar séu aðeins aðgengilegar þeim sem hafa aðgangsheimild.

ógnun: möguleg orsök óæskilegs atviks sem gæti skaðað kerfi eða aðila.

rafrænar undirskriftir: undirskrift í rafrænu formi, viðfest eða skýrlega tengd rafrænum gögnum og notuð er til þess að staðfesta uppruna gagnanna.

raunlægar ráðstafanir: áþreifanlegar öryggisráðstafanir sem ætlaðar eru til að tryggja öryggi aðstöðu, svæðis, búnaðar, upplýsinga eða fólks.

raunlægt öryggi: (e. physical security) ytra öryggi, þ.e. öryggi vélbúnaðar, öryggi aðstöðu, þar sem upplýsingar eru geymdar, vinnsla fer fram eða búnaður er staðsettur, og öryggi athafnasvæðis aðila.

ráðstafanir: sjá öryggisráðstafanir.

rekjanleiki: eiginleikinn sem tryggir að hægt sé að rekja ferli aðgerðar frá upphafi til enda.

réttleiki: trygging á nákvæmni og heilleika upplýsinga og vinnsluaðferða.

réttleiki gagna: eiginleikinn að gögnum hafi ekki verið breytt, bætt við eða eytt á óheimilaðan hátt.

réttleiki kerfis: eiginleikin að kerfi virki eins og til er ætlast skv. kerfislýsingu og ekkert annað.

sannprófun gagna: aðferð til að staðfesta að gögn sem hafa verið vistuð í upplýsinga-kerfum séu í samræmi við þau gögn sem skráð voru inn.

sannvottun: eiginleikinn sem tryggir að auðkenni viðfangsefnis eða tilfangs sé það sem það segist vera. Sannvottun á við einindi eins og notendur, verkferla, kerfi og upplýsingar.

sérréttindi: (e. privilege) hvers kyns fyrirkomulag í fjölnotendakerfi sem gerir notanda kleift að komast framhjá kerfis- og hugbúnaðartálmunum.

spillihugbúnaður: skaðleg forrit, t.d. tölvuveirur, netormar, trójuhestar[1] og röksprengjur.

stjórnkerfi upplýsingaöryggis: (e. information security management system) aðferðir innleiddar til að tryggja öryggi upplýsingaeigna[1] aðila.

stjórnun á samfelldum rekstri: (e. business continuity management) verkferli sem eiga að tryggja að rekstri sé haldið gangandi þó svo að áfall (öryggisfrávik) hafi riðið yfir.

stýringarmarkmið: (e. control objective) þær öryggiskröfur sem taldar eru upp í þessu skjali.

tiltækileiki: eiginleikinn að vera tiltækur og nothæfur samkvæmt eftirspurn einindis með heimild, þ.e. að tryggja notendum með aðgangsheimild aðgang að upplýsingum og tengdum eignum þegar þörf krefur.

trójuhestar: hugbúnaður eða kóði sem er gerður til að hafa áhrif á kerfi með óheimilum hætti og án þess að viðtakandi forritsins hafi óskað eftir því eða taki eftir því.

trúnaður: eiginleikinn að upplýsingar séu ekki aðgengilegar eða birtar óheimiluðum einstaklingum, búnaði eða verkferlum.

upplýsingaeignir: hverjar þær eignir aðila sem varðveita upplýsingar, t.d. rafræn gögn, gögn á pappír, þekking fólks, orðspor aðila og upplýsingar sem fara um samskiptarásir (þ.m.t. símtöl).

upplýsingaþjónusta: veitir aðgang að upplýsingum og upplýsingakerfum, hvort heldur stýrikerfi eða einstökum hugbúnaði.

upplýsingaöryggi: allir þættir sem tengjast því að skilgreina, framfylgja og viðhalda trúnaði[1], réttleika[1], tiltækileika[1], ábyrgðarskyldu, upprunaleika og áreiðanleika[1].

upplýsingaöryggisstefna: reglur, tilskipanir og venjur sem ráða því hvernig eignum, þar á meðal viðkvæmum upplýsingum, sé stjórnað, þær varðar og þeim dreift hjá aðila og á upplýsingakerfum hans.

úttektardagbækur: (e. audit log) skrár þar sem safnað er saman upplýsingum um notkun upplýsingakerfa, þ.m.t. innskráningu notenda, notkun hugbúnaðar, aðgangur að upplýsingum og aðgerðir.

veikleiki: nær yfir varnarleysi eigna(r) sem getur verið afhjúpað af ógnun.

öryggisfrávik: hvert það atvik sem víkur frá settum, skjalfestum öryggisreglum.

öryggisráðstafanir: (e. security control) hver sú aðgerð sem innleidd er til að efla öryggi.

öryggisstefna: sjá upplýsingaöryggisstefna.