Október 2020

Landsarkitektúr upplýsingaöryggis

Útgáfa 0.9

Stjórnarráð Íslands
Fjármála- og efnahagsráðuneytið

Útgefandi:
Fjármála- og efnahagsráðuneytið

Október 2020

fjr@fjr.is

https://www.fjr.is

Umbrot og textavinnsla:
Stjórnarráðið

ISBN 978-9979-820-80-2

Efnisyfirlit

Inngangur

Netöryggi er ein af grunnstoðum stafrænnar opinberrar þjónustu. Tryggja þarf að almenningur og fyrirtæki geti átt í öruggum samskiptum við opinbera aðila og geti treyst því að upplýsingar sem stofnanir hafa yfir að ráða séu vel varðveittar og meðferð þeirra sé með ábyrgum hætti.

Landsarkitektúr um upplýsingaöryggi er ætlað að leiðbeina stofnunum um hvernig þær geti eflt netöryggi og samræmt vinnubrögð og aðgerðir í netöryggismálum þvert á stofnanir. Hann er einn af átta meginköflum í tækniarkitektúr opinberra aðila:

1. Arkitektúr er stjórnað á viðeigandi stigi út frá sameiginlegum ramma
2. Arkitektúr stuðlar að samræmingu, nýsköpun og skilvirkni
3. Arkitektúr og lagaumhverfi styðja hvort annað
4. Öryggi, friðhelgi og trúnaður er tryggður
5. Ferlar á milli opinberra aðila eru skilvirkir og sjálfvirkir
6. Gögnum er deilt á milli opinberra aðila og þau eru endurnýtt
7. Upplýsingatæknilausnir og kerfi vinna hnökralaust saman
8. Gögn eru afhent og þjónusta veitt með áreiðanlegum hætti

Landsarkitektúr um upplýsingaöryggi er því nánari skilgreining á meginkafla fjögur í tækniarkitektúrnum. Vinna við aðra kafla stendur yfir og verða þeir gefnir út eftir því sem verkinu miðar áfram og munu þannig mynda eina heild .

Við gerð landsarkitektúrs um upplýsingaöryggi var horft til þess sem önnur lönd innan Evrópu hafa gert í þessum málaflokki. Mest var horft til Norðurlandanna, þá sérstaklega til Danmerkur.

Gerð Landsarkitektúrs um upplýsingaöryggi fór fram undir stjórn fjármála- og efnahagsráðuneytisins í samvinnu við fulltrúa frá opinberum stofnunum og sveitarfélögum ásamt ráðgjafa í net- og upplýsingaröryggi.

Mikilvægt þótti að fá aðkomu mismunandi aðila til að kortleggja sameiginleg sjónarmið á kröfur til upplýsingaöryggis og var samráðshópurinn skipaður sérfræðingum frá Embætti landlæknis, Háskóla Íslands, Kópavogsbæ, Persónuvernd, Póst- og fjarskiptastofnun, Samgöngustofu, Tryggingastofnun ríkisins og utanríkisráðuneytinu.

Ráðuneytið þakkar fulltrúum í samráðshópi fyrir þeirra miklu vinnu, faglegt og ánægjulegt samstarf í verkefninu.

Fyrirvari

Málefni netöryggis eru kvik og stöðug þróun er í eðli netógna og ráðstöfunum gegn þeim. Þetta rit er gefið út skv. bestu aðferðum sem notaðar eru hverju sinni í heiminum og mun það því taka breytingum eftir því sem mál þróast í framtíðinni. Vert er að taka fram að lög um persónuvernd gera jafnframt kröfu um að persónuupplýsingar séu verndaðar samkvæmt bestu starfsvenjum.

Í byrjun september 2020 tóku gildi lög 78/2019 um um öryggi net- og upplýsingakerfa mikilvægra innviða sem setja kröfur á þá aðila sem reka tækniumhverfi fyrir mikilvæga innviði samfélagsins. Fjöldi stofnana eru í þessum hópi og gerð er ríkari krafa til þeirra hvað netöryggi varðar.

Í kafla 6. er talað um “samningsviðauka sem tekur á rekstraröryggi í samningum við birgja” sem gefin hefur verið út af fjármála- og efnahagsráðuneytinu. Þessi samningsviðauki er nú í vinnslu en hefur ekki endanlega verið gefinn út.

Vakin er athygli á því að í eftirfarandi texta er vísað í hugtökin “viðkvæmar” eða “mjög viðkvæmar” upplýsingar. Skilgreining þessara hugtaka er hins vegar í vinnslu hjá samráðshópi um flokkun upplýsinga á vegum forsætisráðuneytisins. Niðurstöðu þeirrar vinnu er að vænta á árinu 2020 og verður þá texti þessa skjals uppfærður í samræmi við þá flokkun.

Í kafla 8 er rætt um ský og skýjaþjónustu. Unnið er að gerð stefnu og gerð tækniarkitektúrs fyrir skýjaþjónustu hjá ríkinu, sem ætlunin er að gefin verði út í upphafi árs 2021. Þar verður kveðið á um þær kröfur sem gerðar eru til tölvuskýja sem opinberir aðilar nýta sér. Kröfurnar lúta að þeirri þjónustu sem þar verður í boði, samræmdum innkaupum, en ekki síst þeim kröfum sem gerðar eru til öryggis þessa umhverfis.

Ritið verður uppfært m.t.t. þessa eftir því sem þurfa þykir.

1. Stjórnkerfi upplýsingaöryggis

Það er mikilvægt að allir opinberir aðilar innleiði stjórnkerfi upplýsingaöryggis byggt á alþjóðlega staðlinum ISO/IEC 27001 en með því er hægt að auka rekstraröryggi þeirra. Mikilvægt er að stjórnkerfið nái utan um allan rekstur viðkomandi aðila en takmarkist ekki við upplýsingatæknideildir. Allir opinberir aðilar þurfa að hafa innleitt stjórnkerfi upplýsingaöryggis byggt á þessum staðli fyrir lok ársins 2022. Þeir aðilar sem eru hluti af nauðsynlegum innviðum landsins, þ.e.a.s. þeir sem falla undir lög 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða og þeir sem meðhöndla upplýsingar sem eru flokkaðar sem mjög viðkvæmar þurfa að hljóta faggilda vottun á öryggisstjórnkerfi sínu fyrir lok ársins 2022. Ekki er gerð krafa um vottun hjá öðrum opinberum aðilum. Opinberir aðilar skulu hafa skjalfesta öryggisstefnu, sem er samþykkt af æðstu stjórnendum. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda til öryggismála. Við mótun öryggisstefnu skal taka mið af því hversu mikla vernd upplýsingar þurfi, hvernig skuli vernda þær og þeirri aðferð sem viðhöfð verður við vinnslu þeirra.

Mikilvægur þáttur af innleiðingu stjórnkerfis upplýsingaöryggis snýr að því að úthluta ábyrgð á upplýsingaöryggi til viðeigandi starfsmanna. Gerð er sú krafa að þeir opinberu aðilar sem meðhöndla viðkvæmar og mjög viðkvæmar upplýsingar hafi upplýsingaöryggisstjóra. Mikilvægt er að upplýsingaöryggisstjórar hljóti ákveðna grunnþjálfun í upplýsingaöryggi. Upplýsingaöryggisstjórar opinberra aðila sem meðhöndla viðkvæmar og mjög viðkvæmar upplýsingar þurfa að hafa viðurkennda vottun á þekkingu sinni. Eftirfarandi vottanir teljast ásættanlegar: Meistara gráða í upplýsingaöryggi, CISSP (Certified Information Systems Security Professional) – IISSCC, CISM (Certified Information Security Manager) – ISACA og CCISO (Certified Chief Information Security Officer) – ECCouncil.

2. Áhættustjórnun

Þegar kemur að upplýsingaöryggi þá skiptir miklu máli að taka upplýstar ákvarðanir með tilliti til þekktrar áhættu. Opinberir aðilar þurfa að innleiða formlegt ferli við framkvæmd áhættumats og áhættumeðferðar þar sem ásættanleg áhætta er skilgreind. Opinberir aðilar sem meðhöndla viðkvæmar og mjög viðkvæmar upplýsingar þurfa að framkvæma áhættumat fyrir starfsemi sína að lágmarki einu sinni á ári. Aðrir opinberir aðilar þurfa að framkvæma áhættumat að lágmarki annað hvert ár. Í framhaldi af áhættumati skal skjalfesta áætlun um hvernig eigi að meðhöndla áhættuþætti sem bera meira en ásættanlega áhættu. Í áhættumati skal taka tillit til raunlægra áhættuþátta (e. Physical security), stafrænna þátta og hugsanlega annarra þátta. Í áætlun um meðferð áhættu skal úthluta ábyrgðaraðilum ábyrgð á öryggisráðstöfunum og tímasetja hvenær áætluðum úrbótum skal vera lokið. Æðstu stjórnendur skulu fylgja úrbótaáætluninni eftir.

Æskilegt er að taka tillit til innri ógna við framkvæmd áhættuamts.

3. Lykilverklagsreglur

Undirstaða þess að tryggja rekstraröryggi, leynd, réttleika, tiltækileika og rekjanleika er að opinberir aðilar innleiði lykilöryggisþætti til að styðja sína öryggisstefnu. Athugið að eftirfarandi kröfur eru hugsaðar sem lágmarkskröfur. Þeir aðilar sem meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar eru hvattir til þess að gera auknar kröfur.

3.1 Stjórnun aðgangs

Opinberir aðilar skulu innleiða formlegt ferli og verklagsreglur til að stjórna aðgangi að lykilupplýsingakerfum sínum. Þar sem meðal annars kemur fram hverjir geta óskað eftir því að stofnaður verði nýr aðgangur, aðgangi breytt eða lokað. Ferlið skal samþykkt af stjórnendum, það skal vera rekjanlegt og skoðað til samþykktar að lágmarki einu sinni á ári sem hluti af innra eftirliti. Þar sem því verður við komið skal styðjast við aðgangshópa. Framangreint minnkar líkur á að aðgangsheimildir fylgi starfsmönnum þegar þeir flytja sig á milli starfa og styður aðskilnað starfa.

Ábyrgðarmenn upplýsingakerfa skulu rýna aðgang að sínum kerfum að lágmarki einu sinni á ári.

Opinberir aðilar skulu tryggja örugga auðkenningu og sannvottun ytri aðila að kerfum sínum og gögnum. Stofnanir sem veita þjónustu til almennings og fyrirtækja skulu nýta aðgangsstýringu sem uppfyllir kröfur skv. lögum nr. 5521/2019 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti. Stofnanir skulu nýta lausnir sem styðja við rafræn skilríki, sem gefin eru út undir rótarskilríkinu Íslandsrót[1] sem er í eigu ríkisins.

3.2 Öryggisuppfærslur

Opinberir aðilar skulu innleiða og vinna eftir formlegu ferli fyrir vöktun og uppsetningu á öryggisuppfærslum fyrir lykilhugbúnað, öll stýrikerfi og netbúnað. Opinberir aðilar bera ábyrgð á að settar séu inn mikilvægar (e. critical) öryggisuppfærslur án ónauðsynlegra tafa eftir að þær hafa verið gefnar út af framleiðendum en þó eigi síðar en sjö dögum eftir útgáfu þeirra.

Aðrar öryggisuppfærslur skulu settar upp innan 90 daga frá því að þær eru gefnar út. Óheimilt er að nota hugbúnað eða stýrikerfi sem framleiðandi er hættur að styðja með öryggisuppfærslum. Opinberir aðilar þurfa að vakta stöðu öryggisuppfærslna á miðlurum og vinnustöðvum. Innra eftirlit skal taka út stöðu öryggisuppfærslna að lágmarki einu sinni á ári.

[1] https://www.islandsrot.is/

3.3 Veikleikagreiningar og innbrotsprófanir

Opinberir aðilar skulu innleiða og vinna eftir formlegu ferli varðandi framkvæmd á veikleikagreiningu net- og upplýsingakerfa sinna. Mikilvægt er að lykilupplýsingakerfi séu hluti af veikleikagreiningu. Þeir aðilar sem meðhöndla viðkvæmar og mjög viðkvæmar upplýsingar skulu framkvæma slíkar greiningar að lágmarki ársfjórðungslega. Aðrir skulu framkvæma þær að lágmarki einu sinni á ári. Opinberir aðilar skulu bregðast við veikleikum sem finnast og koma þeim í úrbótaferli. Niðurstöður veikleikagreininga og stöðu á framkvæmd úrbóta skal kynna fyrir æðstu stjórnendum. Það skal gerast sem hluti af innra eftirliti. Þeir opinberu aðilar sem vinna með viðkvæmar eða mjög viðkvæmar upplýsingar skulu framkvæma innbrotsprófanir að lágmarki annað hvert ár.

3.4 Atvikastjórnun (e. Incident Management)

Opinberir aðilar skulu innleiða og vinna eftir formlegu ferli við atvikastjórnun. Verklagið skal kynna öllum starfsmönnum og skulu þeir hvattir til að tilkynna öryggisatvik sem og frávik frá verklagsreglum. Upplýsingum um atvik og frávik skal haldið til haga i stafrænni skrá. Stjórnendur skulu reglulega fara yfir helstu öryggisatvik og frávik sem hafa verið tilkynnt og taka afstöðu til þess hvort og hvernig skuli bregðast við þeim. Ferli fyrir stjórnun atvika skal tekið út að minnsta kosti einu sinni á ári sem hluti af innra eftirliti.

Opinberir aðilar sem falla undir lög nr. 78/2019 um net og upplýsingaöryggi mikilvægra innviða skulu innleiða sem hluta af atvikastjórnunarferli að tilkynna öryggisatvik til CERT-IS í samræmi við þau viðmið sem sett eru í lögunum.

3.5 Innbrotsvöktunarkerfi (e. Intrusion Detection System / Intrusion Prevention System)

Opinberir aðilar sem meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar skulu koma á formlegu ferli fyrir tölvuinnbrotsvöktun og/eða aðgerðir til að fyrirbyggja tölvuinnbrot með notkun tölvuinnbrotsvöktunarkerfis (IDS/IPS). Mikilvægt er að fylgjast með tilkynntum atvikum í tölvuinnbrotsvöktunarkerfinu að lágmarki einu sinni á dag. Innbrotsvöktunarkerfið skal a.m.k. ná til lykil upplýsingakerfa og innviða.

3.6 Öryggisafritunartaka (e. Backup)

Opinberir aðilar skulu koma á og vinna eftir formlegu ferli fyrir töku öryggisafrita og endurheimt lykilupplýsingakerfa og -gagna. Verklagið skal vera samþykkt formlega af æðstu stjórnendum. Umfang öryggisafritunartöku skal ná til lykilupplýsingakerfa og -gagna. Æskilegt er að prófa endurheimt þeirra að lágmarki einu sinni á ári og það skal gera á rekjanlegan hátt.

3.7 Gagnaflutningur

Opinberir aðilar skulu tryggja öruggan flutning gagna og koma á og vinna eftir formlegu ferli varðandi flutning og meðferð þeirra. Þær skulu tryggja rekjanleika í flutningi gagna á hvaða formi sem þau eru og tryggja leynd og réttleika

viðkvæmra gagna með dulritun þeirra eða tryggja fiktvarnir (e. tamper proof) ef þau eru á öðru formi. Verklagið skal vera samþykkt formlega af æðstu stjórnendum.

Stofnanir skulu nýta Strauminn[2] (e. X-Road) til rafræns gagnaflutnings sín á milli, sé hann á milli netkerfa (gögn eða kerfi ekki vistuð á sama neti eða í sama tækniumhverfi). Heilbrigðisstofnanir nýta jafnframt Heklunet og Heklugátt til flutnings heilbrigðisgagna.

Æskilegt er að gera úttekt á gagnaflutningsferlum og -kerfum að lágmarki einu sinni á ári og það skal gera á rekjanlegan hátt.

Stofnanir skulu að tryggja að allar vefsíður út á internetið nýti HTTPS (Hypertext Transfer Protocol Secure) og TLS (Transport Layer Security) dulkóðun.

3.8 Innleiðing nýrra kerfa, hugbúnaðar og forrita

Þeir opinberu aðilar sem eru að meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar skulu innleiða og vinna eftir formlegu ferli varðandi innleiðingu á nýjum kerfum, hugbúnaði og forritum sem tengjast net- og upplýsingakerfum þeirra.

Framkvæma skal veikleikagreiningu og áhættumat fyrir þau kerfi, hugbúnað og forrit sem til stendur að innleiða og staðfesta að lágmarkskröfur um öryggi séu uppfylltar. Standist kerfi / hugbúnaður / forrit ekki lágmarkskröfur skal ekki taka það í notkun án viðeigandi ráðstafana til að tryggja öryggi annarra kerfa. Heimilt er að framkvæma veikleikagreiningu og áhættumat samhliða mati á áhrifum á persónuvernd, ef það á við.

Ef búið er að framkvæma veikleikagreiningu á hugbúnaði af öðrum aðila er ásættanlegt að styðjast við þá veikleikagreiningu og ekki þörf á því að endurtaka úttektina að því gefnu að úttektin hafi verið framkvæmd innan 18 mánaða. Þegar niðurstöður úttekta annarra eru notaðar skal vísa í gögn um hverjir framkvæmdu úttektina, hvenær, umfang hennar og niðurstöður.

3.9 Breytingastjórnun

Opinberir aðilar sem meðhöndla viðkvæmar og mjög viðkvæmar upplýsingar skulu vinna eftir formlegu ferli fyrir stjórnun meiriháttar breytinga og þeirra breytinga sem gætu haft mikil áhrif á rekstraröryggi. Í ferlinu skal koma fram:

- hver þarf að samþykkja breytingar
- hverju á að breyta
- hvenær fyrirhuguð breyting mun eiga sér stað
- hver er áætlaður tími sem fer í breytingarnar og/eða mögulegur tími sem þjónusta liggur niðri

[2] https://stafraent.island.is/verkefni/straumurinn/

- hverjir munu framkvæma viðkomandi breytingu
- hvernig verði brugðist við ef breyting mistekst (t.d. ef endurheimta þarf kerfi frá öryggisafriti)
- hversu mikill tími fer í að hætta við breytingar, t.d. ef endurheimta þarf kerfi (komi fram villur)
- hvernig breytingar verða prófaðar

Ferlið skal vera tekið út að lágmarki einu sinni á ári sem hluti af innra eftirliti.

Mikilvægt er að framkvæma áhættumat fyrir allar stærri breytingar þar sem meðal annars er metið hvort viðkomandi breyting geti haft áhrif á önnur upplýsingakerfi eða aðra aðila. Ef svo er þá er æskilegt að upplýsa viðkomandi hagsmunaaðila um fyrirhugaðar breytingar. Æskilegt er að hafa í huga að sumar tímasetningar geta verið óheppilegar fyrir stórar breytingar t.d. mánaðarmót.

3.10 Ráðningar

Opinberir aðilar skulu vinna eftir formlegu ferli við ráðningar starfsmanna og verktaka sem og þeim lögum og reglum sem gilda um veitingu starfa hjá ríkinu. Skoðun á bakgrunni umsækjenda skal vera hluti ráðningarferlis þegar starf tengist rekstri net- og upplýsingakerfa sem og fyrir starfsmenn sem munu fá aðgang að viðkvæmum upplýsingum. Einnig skal afla sömu upplýsinga, eða fara fram á að þeirra sé aflað, fyrir starfsmenn þjónustuaðila og verktakafyrirtækja sem munu fá aðgang að innviðum eða viðkvæmum upplýsingum. Sem hluti af bakgrunnsskoðun skal taka afstöðu til eftirfarandi þátta eftir því sem við á:

- Staðfesta menntun viðkomandi
- Fá afrit af sakavottorði viðkomandi
- Hafa samband við tvo meðmælendur / fyrri atvinnuveitendur

Við skoðun á bakgrunni umsækjanda þarf að öðru leyti að fara eftir lögum nr. 70/1995 um réttindi og skyldur starfsmanna ríkisins og lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga.

3.11 Trúnaðaryfirlýsingar

Allir starfsmenn og verktakar opinberra aðila sem hafa aðgang að trúnaðarupplýsingum, viðkvæmum persónuupplýsingum, þróun kerfa eða koma að rekstri neta eða upplýsingakerfa skulu undirrita sérstaka trúnaðaryfirlýsingu / þagnarskylduyfirlýsingu. Í þeim tilfellum sem um verktaka er að ræða, þá er ásættanlegt að tekið sé á trúnaðaryfirlýsingum í samningi við fyrirtæki, þ.e. að fyrirtæki ábyrgist að allir starfsmenn þess skrifi undir trúnaðaryfirlýsingar.

3.12 Þjálfun starfsmanna og verktaka

Opinberir aðilar skulu stuðla að góðri öryggisvitund eigin starfsmanna og verktaka með reglulegum námskeiðum og/eða starfsmannaþjálfun þar sem

fjallað er um helstu þætti er tengjast upplýsingaöryggi. Æskilegt er að starfsmenn sæki slíkt námskeið að lágmarki einu sinni á ár.

Mikilvægt er að þeir aðilar sem reka upplýsingakerfi opinberra aðila hafi hlotið þjálfun í því að tryggja öryggi þeirra upplýsingakerfa sem þeir bera ábyrgð á að reka og viðhalda. Þeir aðilar sem reka upplýsingakerfi opinberra aðila sem meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar skulu hafa hlotið viðurkennda vottun á því að kunna að tryggja öryggi þeirra kerfa sem þeir eru að reka. Dæmi um vottanir: Cisco Certified Networking Associate Security, Microsoft 365 Certified Security Administrator og/eða Red Hat Certified Specialist in Security: Linux

3.13 Starfslok

Opinberir aðilar skulu vinna eftir formlegu ferli við starfslok starfmanna hvað varðar aðgang að gögnum og upplýsingum. Að öðru leyti fer um starfslok samkvæmt lögum um réttindi og skyldur starfsmanna ríkisins. Í formlegu ferli við starfslok felst að skilgreina þarf verklag um lokun (og mögulega eyðingu) á aðgangi starfsmanna og verktaka sem hætta störfum. Mikilvægt er að tryggja skilvirkt samstarf á milli upplýsingatækni- og mannauðssviðs. Æskilegt er að mannauðssvið / þeir sem bera ábyrgð á mannauðsmálum tilkynni upplýsingatæknisviði / þeim sem bera ábyrgð á upplýsingatækni um leið og vitað er um áætluð starfslok þannig að hægt sé að setja tímamörk á aðgang að upplýsingakerfum þar sem því verður við komið. Ef starfsmaður er með öryggisvottun Ríkislögreglustjóra þarf að tilkynna Ríkislögreglustjóra um að viðkomandi þurfi hana ekki lengur. Æskilegt er að taka viðkomandi af öllum póstlistum, fjarlægja viðkomandi úr öllum aðgangshópum og loka pósthólfi í síðasta lagi 14 dögum eftir síðasta starfsdag og að öðrum ákvæðum reglna um rafræna vöktun sé fylgt í hvívetna. Mikilvægt er að búnaði sem hefur innihaldið viðkvæmar upplýsingar sé skilað við starfslok.

4. Áætlun um samfelldan rekstur

Opinberir aðilar sem meðhöndla viðkvæmar og mjög viðkvæmar upplýsingar skulu innleiða og vinna eftir formlegu ferli fyrir samfelldan rekstur. Ferlið skal byggja á bestu starfsvenjum og alþjóðlegum stöðlum. Kortleggja skal viðbrögð við helstu áhættuþáttum sem geta valdið rekstrarrofi / rofi í rekstri og forgangsraða endurheimt kerfa og gagna. Prófa skal áætlun um samfelldan rekstur á rekjanlegan hátt að lágmarki árlega.

Mikilvægt er að taka tillit til mögulegra stóráfalla í áætlun um samfelldan rekstur eða útbúa sérstaka viðbragðsáætlun vegna stóráfalla. Áætlunin skal ná til lykilþjónustu, sem aðilarnir veita auk lykilupplýsingakerfa þeirra. Hana skal kynna æðstu stjórnendum og skulu þeir samþykkja hana formlega, bæði áætlaðan tíma og hámarkstíma sem það muni taka að endurheimta kerfi og þjónustur.

Mikilvægt er að taka tillit til áætlunar um samfelldan rekstur í breytingastjórnunarferli. Ef möguleiki er að viðkomandi breyting geti haft áhrif á sjálfa áætlunina eða áætlaðan endurheimtartíma, skal uppfæra áætlun um samfelldan rekstur í samræmi við það.

5. Innra eftirlit

Til þess að tryggja rekstraröryggi þarf að hafa virkt innra eftirlit. Opinberir aðilar skulu vinna eftir formlegu ferli um innra eftirlit þar sem lykilferli og verklagsreglur skulu teknar út að lágmarki annað hvert ár. Þeir opinberu aðilar sem meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar skulu framkvæma innri úttektir á lykilferlum og verklagsreglum að lágmarki árlega. Mikilvægt er að það sé hægt að rekja þessar úttektir og að öll frávik sem finnast séu skráð samkvæmt verklagsreglu um frávikaskráningu. Helstu niðurstöður innri úttekta skulu kynntar æðstu stjórnendum með reglulegum hætti.

6. Stjórnun birgja

Til þess að tryggja rekstraröryggi opinberra aðila skiptir miklu máli að taka á kröfum um rekstraröryggi í samningum við birgja. Fjármála- og efnahagsráðuneytið hefur gefið út samningsviðauka sem tekur á rekstraröryggi í samningum við birgja. Opinberir aðilar sem meðhöndla ekki viðkvæmar eða mjög viðkvæmar upplýsingar geta haft samningsviðaukann til hliðsjónar þegar þeir semja við sína birgja. Opinberir aðilar sem meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar þurfa að taka upp þennan samningsviðauka við þá birgja sem sjá um rekstur upplýsingakerfa sem innihalda slíkar upplýsingar eða eru að vinna með slíkar upplýsingar fyrir þeirra hönd. Æskilegt er að opinberir aðilar hafi yfirsýn yfir birgja og undirbirgja t.d. í þeim tilfellum þar sem um keðjuútvistun er að ræða.

6.1 Eftirlit með birgjum

Opinberir aðilar sem meðhöndla viðkvæmar eða mjög viðkvæmar upplýsingar skulu óska eftir skýrslu að lágmarki árlega frá sínum birgjum með upplýsingum um niðurstöður innra eftirlits þeirra þátta sem koma fram í samningsviðaukanum sem fjármála- og efnahagsráðuneytið gaf út. Helstu niðurstöður skal kynna fyrir æðstu stjórnendum.

7. Persónuvernd

Öll vinnsla persónuupplýsinga hjá stjórnvöldum þarf að samrýmast lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga, þ.m.t. að setja sér persónuverndarstefnu, framkvæma mat á áhrifum á persónuvernd (MÁP), setja sér verklagsreglur um tilkynningar um öryggisbresti og hafa persónuverndarfulltrúa.

Ef stjórnvald eða þjónustuaðili (sem og undirverktakar) þess hyggst vinna með persónuupplýsingar utan íslenskrar lögsögu þarf að fara að ákvæðum V. kafla reglugerðar (ESB) 2016/679 og gera viðeigandi ráðstafanir. Flutningur persónuupplýsinga innan EES, og til þeirra ríkja sem hafa verið metin örugg þriðju lönd, er almennt talinn heimill án viðbótarráðstafana.

Ef stjórnvald vinnur með mikið magn persónuupplýsinga og/eða mikið magn viðkvæmra persónuupplýsinga getur þurft að huga að því að stjórnvaldið fái sérstaka persónuverndarvottun eða að stjórnvöld sameinist um hátternisreglur við vinnslu persónuupplýsinga en að svo stöddu er ekki lögð sú skylda á stjórnvöld.

Rétt er að hafa í huga að stjórnkerfi upplýsingaöryggis og persónuvernd eiga ýmislegt sameiginlegt. Því geta ýmis verkfæri nýst við að ná fram reglufylgni við bæði. Hins vegar er rétt að hafa í huga að persónuverndarlöggjöfin snýr ekki eingöngu að stjórnkerfi upplýsingaöryggis heldur einnig að því t.d. hvort fullnægjandi heimildir séu til staðar fyrir vinnslu og að meginreglum um vinnslu persónuupplýsinga sé fylgt. Því þarf ávallt að leggja sjálfstætt mat á þær aðgerðir sem nauðsynlegt er að grípa til út frá ákvæðum persónuverndarlaga og þær aðgerðir sem hér er mælt fyrir um.

Athugið að hægt er að finna nánari upplýsingar og leiðbeiningar á vefsíðu Persónuverndar.

8. Ský og skýjaþjónusta

Mikilvægt er að nota aðeins þær skýjaþjónustur sem Ríkiskaup hefur samþykkt. Ávallt skal ganga úr skugga um að gögn séu vistuð innan evrópska efnahagssvæðisins. Tryggja þarf að allar helstu öryggisstillingar séu virkjaðar og að viðkomandi skýjalausn hafi fengið vottun á upplýsingaöryggi. Mikilvægt er að þeir sem sjá um rekstur á viðkomandi skýjalausn hafi fagþekkingu á því hvernig hægt sé að virkja helstu öryggisstillingar.

Að öðru leyti eiga sömu reglur við um eftirlit með skýjaþjónustuveitendum og með birgjum.

9. Hugbúnaðarþróun

Þeir opinberu aðilar sem þróa hugbúnað sem meðhöndlar viðkvæmar upplýsingar skulu uppfylla eftirfarandi kröfur.

9.1 Formlegt ferli við hugbúnaðarþróun

Vinna skal eftir formlegu ferli við hugbúnaðarþróun sem byggir á bestu starfsvenjum. Æskilegt er að horfa til alþjóðlegra staðla þegar kemur að öryggi í hugbúnaðarþróunarferlinu, t.d. ISO/IEC 27034. Tryggja skal að a.m.k. einn forritari í hverju hugbúnaðarþróunarverkefni hafi hlotið þjálfun í öruggri hugbúnaðarþróun og allir starfsmenn sem að verkefninu koma séu meðvitaðir um öryggiskröfur til hugbúnaðarþróunar.

9.2 Huga að persónuvernd við þróun

Mikilvægt er að huga að lögum um persónuvernd frá upphafi þegar teknar eru í notkun nýjar hugbúnaðarlausnir. Persónuverndarlögin gera ráð fyrir að persónuvernd sé bæði innbyggð og sjálfgefin í öllum nýjum hugbúnaði. Innbyggð persónuvernd felur í sér að ráðstafanir eru innbyggðar í hugbúnað, upplýsingakerfi og vinnslu frá upphafi og eru hannaðar til að fylgja meginreglum persónuverndar. Sjálfvirk persónuvernd felur í sér að sjálfgefið sé að eingöngu nauðsynlegar upplýsingar séu unnar og ekki umfram það og að tekið sé tillit til eðli, umfangs, samhengis og tilgangs vinnslu þegar unnið er með persónuupplýsingar.

Nánar um þær kröfur sem gerðar eru til persónuverndarráðstafana við þróun hugbúnaðar.

Opinberir aðilar þurfa því að kortleggja hvaða upplýsingar er nauðsynlegt að vinna með til að geta sinnt lögbundnum verkefnum sínum auk þess þarf að ákveða hvaða ráðstafanir eru nauðsynlegar til að tryggja að meginreglum persónuverndarlaganna sé fylgt. Þá þurfa opinberir aðilar einnig að kortleggja hvaða réttindi einstaklinga eigi við um þeirra vinnslu og að hugbúnaðurinn geti mætt þeim réttindum, t.a.m. ef einstaklingur óskar eftir aðgangi að upplýsingum um sig o.fl.

9.3 Fullvissa við sannvottun á rafrænum auðkennum

Rafræn auðkenni geta verið margskonar, meðal annars notandanafn og lykilorð (þ.m.t. veflyklar), einskiptisaðgangsorð (oft með auðkennislyklum), kóðar í farsíma og rafræn skilríki (vottorð).

Aðferðir við sannvottun á rafrænum auðkennum við innskráningu skulu taka mið af mögulegum skaða vegna rangrar auðkenningar og tryggja viðunandi varnir gegn innbrotum og fölsun á kennslum. Það er mikilvægt að ákvarða kröfur til styrkleika rafrænna auðkenna, en jafnframt skal gera viðeigandi ráðstafanir til að verjast ógnum við notkun þeirra, auk almennra ógna við sannvottun kennsla svo

sem spillihugbúnaði, bragðvísi (e. social engineering), mistökum notenda, innbrotum í samskipti við sannvottun og veikleikum í verklagi.

Við hönnun kerfa skal huga að lagskiptum stýringum (e. security in depth) með hliðsjón af rekstrarumhverfi, notendahugbúnaði og kröfum um fullvissu í sannvottun kennsla.

Fullvissustig (e. assurance level) við sannvottun á kennslum fer eftir því hversu mikil tiltrú er á kennslum notandans sem óskar innskráningar, með hliðsjón af ferlum fyrir sannprófun og sannvottun kennslanna, styrkleika auðkennanna og þeim tæknilegu stýringum sem beitt er við innskráningu. Við ákvörðun á kröfum um fullvissustig skal taka mið af ákvæðum í lögum nr. 55/2019 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti.

9.4 Örugg samskipti og vistun gagna

Sá hugbúnaður sem meðhöndlar viðkvæmar eða mjög viðkvæmar upplýsingar skal styðja dulkóðaðar gagnasendingar innan kerfis og milli kerfa. Mikilvægt er að viðkvæmar upplýsingar séu einungis sendar dulkóðaðar eða yfir dulkóðuð samskipti. Mikilvægt er að vista aldrei lykilorð á texta formi heldur nota alþjóðlega viðurkenndar starfsvenjur eins og tætifall og salt. Nánari upplýsingar er hægt að finna í nýjustu útgáfu OWASP Top 10. Æskilegt er að tryggja að viðkvæm gögn séu dulkóðuð við hvíld (e. at rest).

9.5 Stjórnun öryggisveikleika

Þegar öryggisgallar finnast í hugbúnaði sem er þróaður af opinberum aðila skal tilkynna hagsmunaaðilum um öryggisveikleikann eins fljótt og mögulegt er og án ónauðsynlegra tafa. Ásamt upplýsingum um fyrirhuguð viðbrögð (ef einhver eru) og leiðbeiningum um hvernig hægt sé að lágmarka eða fyrirbyggja áhættu tengda öryggisveikleikanum. Mikilvægt er að upplýsa upplýsingaöryggisstjóra um alla alvarlega öryggisveikleika.