ÖRYGGISHANDBÓK ÞJÓNUSTUAÐILA

Leynd

Réttleiki

Tiltækileiki

ISO

Útgáfa 9

VERITAS

EFNISYFIRLIT

1. Formáli

Veritas Capital hf. er móðurfélag þjónustufyrirtækja í lyfja- og heilbrigðis-geiranum. Félagið er kjölfesta samstæðunnar og veitir þjónustu til dóttur-fyrirtækjanna svo þau geti einbeitt sér að kjarnastarfsemi sinni. Hér eftir stendur Veritas fyrir móðurfélagið og öll dótturfélög.

Öryggismál verða sífellt mikilvægari, sér í lagi á sviði upplýsingatækni. Meiri upplýsingar eru varðveittar á tölvutæku formi í dag og tækni eins og Internetið og tölvupóstur ýta undir þá þróun. Innan Veritas eru varðveitt ýmis gögn sem varða ekki aðeins okkar eigið fyrirtæki og starfsfólk, heldur einnig viðskiptavini fyrirtækisins.

Margar hættur steðja að hvers kyns upplýsingum. Lög um meðferð og notkun á upplýsingum eru strangari en áður var, tölvuþrjótar verða sífellt kænni og við eins og aðrir þurfum að gera ráðstafanir vegna þessa.

Þessir þættir leiða allir til einnar niðurstöðu – við verðum að sýna mikla aðgæslu og huga vel að öryggi upplýsinga. Þar sem Veritas hlítir verklagi sem grundvallast á ISO 27001 upplýsingaöryggis staðlinum er það mjög mikilvægt að þjónustuaðilar kynni sér efni þessa skjals vel.

Þjónustuaðilar þurfa að staðfesta að þeir hafi lesið þær reglur sem fram koma í skjalinu, með því að undirrita „trúnaðarskuldbindingu þjónustu-aðila“ með tilvísun í þetta skjal.

Hrund Rudolfsdóttir, forstjóri

2. Inngangur

2.1. *Hlutverk birgja/verktaka/Þjónustuaðila í upplýsingaöryggi hjá Veritas*

Hjá Veritas er unnið með upplýsingar sem eru allt frá því að vera almennar upp í það að vera viðkvæmar sem eiga ekki erindi út fyrir fyrirtækið. **Leynd, réttleiki og tiltækileiki** þessara upplýsinga skiptir eigendur þeirra höfuðmáli og ber Veritas að vernda þær gegn hvers kyns misnotkun. Birgjar/verktakar/þjónustuaðilar *(hér eftir nefndir þjónustuaðilar)* taka þátt í að verja gögn sem Veritas vinnur með og varðveitir.

Þjónustuaðilar eins og starfsmenn verða að fara eftir þeim reglum sem hafa verið settar um meðhöndlun gagna og vinnu við upplýsinga-vinnslubúnað. Ábyrgð þjónustuaðila er mikil þegar þeir sinna þjónustu-beiðnum fyrir Veritas þar sem einföld mistök geta valdið truflun á starfsemi fyrirtækisins og valdið viðskiptavinum alvarlegum truflunum.

Í þessari handbók hafa verið teknar saman helstu reglur sem snúa að þjónustuaðilum sem vinna við upplýsingatækni eða gögn fyrir Veritas. Ef þjónustuaðili er ekki viss skal hann leita aðstoðar starfsmanna Veritas til þess að ganga úr skugga um hvaða reglur gilda hverju sinni.

Þjónustuaðilar skulu hafa í huga að aðgerðir sem framkvæmdar eru án undirbúnings eða nægrar þekkingar á viðfangsefninu geta valdið truflun eða stöðvun á starfsemi Veritas. Öll slík truflun hefur áhrif á áreiðanleika og orðspor fyrirtækisins fyrir utan fjárhagslegt tjón sem truflun getur haft í för með sér.

2.2. *Stefna Veritas í upplýsingaöryggismálum*

Veritas fylgir eftirfarandi upplýsingaöryggisstefnu sem tekur mið af ISO/IEC 27002 Starfsvenjur fyrir stjórnun upplýsingaöryggis.
Stefnuna er hægt að nálgast á heimasíðu Veritas.

2.3. *Hvað er Upplýsingaöryggisnefnd?*

Upplýsingaöryggisnefnd ber ábyrgð á því að stjórna innleiðingu, eftirfylgni og réttri notkun öryggisreglna um upplýsingatæknimál ásamt öryggisstöðlum og aðferðum sem styðja við þær. Nefndin er aðal tengi-liður við notendur vegna atriða sem snerta öryggi upplýsinga Veritas.

Nefndin gerir viðeigandi ráðstafanir í samræmi við reglur og öryggisstaðla þegar öryggisrof er tilkynnt. Tilkynningar skulu sendar til upplýsinga-öryggisstjóra á netfangið oryggi@veritas.is.

2.4. *Hverjir eru í nefndinni?*

Í Upplýsingaöryggisnefnd eru:

- Fjármálastjóri Veritas
- Deildarstjóri upplýsingatæknideildar (UTD)
- Gæða- og upplýsingaöryggisstjóri Veritas

2.5. *Ábyrgð*

Ábyrgð á öryggismálum er endanlega hjá forstjóra en Upplýsingaöryggis-nefnd ber ábyrgð á eftirliti og þróun upplýsingaverndar.

2.6. *Tilkynningarskylda*

Verði þjónustuaðili var við öryggisatvik eða vakni grunur um öryggisatvik ber honum skylda til að tilkynna þau. Sem hluta af verkefnum sínum fyrir Veritas geta þjónustuaðilar komist að veikleikum í kerfum fyrirtækjanna og því er mikilvægt að þeir tilkynni slík atvik strax til upplýsingaöryggisstjóra.

3. Upplýsingaöryggi fyrir þjónustuaðila

3.1. *Öryggisreglur*

Þeim öryggisreglum sem tilgreindar eru hér á eftir ber að fylgja.

3.2. *Móttaka og brottför þjónustuaðila*

Þjónustuaðilar eiga almennt að tilkynna komu sína og skal starfsmaður Veritas taka á móti þeim. Við brottför skal starfsmaður Veritas fylgja þjónustuaðila til dyra. Þessar reglur gilda ekki um þjónustuaðila sem hafa sér aðgangskort.

3.3. *Reglur um tölvur*

Tölvur sem Veritas leggur þjónustuaðilum til eru ætlaðar til að nota í þágu fyrirtækisins og önnur notkun er ekki leyfileg. Það sem unnið er á tölvurnar er eign fyrirtækisins. Séu verk sem falla undir lög um höfundarrétt unnin á tölvubúnað fyrirtækisins áskilur fyrirtækið sér allan rétt til að nýta það að fullu nema um annað sé samið fyrirfram. Veritas leggur til allan hugbúnað sem settur er á tölvur fyrirtækisins og uppsetningu hans annast starfsmenn upplýsingatæknideildar (UTD) Veritas. Starfsmenn UTD sjá um að tengja tölvurnar saman í net þar sem það á við og sjá um að tengja það við önnur net, t.d. Internetið.

- Þjónustuaðilum, öðrum en þeim sem til þess eru ráðnir, er óheimilt að setja upp hugbúnað á tölvur Veritas. Það er með öllu óheimilt að setja ólöglegan hugbúnað á tölvur fyrirtækisins. Ólöglegur hugbúnaður er m.a. sá hugbúnaður sem ber að greiða leyfisgjald fyrir en hefur ekki verið gert.
- Þjónustuaðilum ber að skrá og vista skjöl sem varða skráð samskipti eða mál sem eru í vinnslu. Skjöl þessi þarf að vernda og varðveita sem sönnunargögn um atburðarrás.
- Þjónustuaðilum ber að „taka til“ eftir sig og fjarlægja ónauðsynleg eða úrelt gögn úr gagnageymslum Veritas.

3.4. *Reglur um notkun á Internetinu*

Þjónustuaðilar geta fengið aðgang að Internetinu um gáttir netkerfisins. Aðgangurinn er eingöngu ætlaður til að afla upplýsinga sem að gagni koma við þau verkefni sem þjónustuaðili vinnur að fyrir Veritas. Eftirfarandi reglur gilda um notkun Internettengingar:

- Fyrirtækið áskilur sér rétt til að skrá alla notkun á Internetinu í þeim tilgangi að fylgjast með að reglum þessum sé fylgt og til að tryggja sem hagkvæmasta notkun netsins og uppfylla nauðsynlegar öryggis-kröfur.
- Notendur sem nota tengingu fyrirtækisins við Internetið skulu vera vel á verði við val á vefsetrum sem þeir skoða. Aðgangur að óviðeigandi síðum sem tengjast ekki starfinu er óheimill jafnt á skrifstofutíma sem utan hans.
- Notkun tenginga fyrirtækisins við Internetið í einkaþágu er ekki leyfð.
- Óheimilt er að sækja hugbúnað á Internetið nema þann sem nauðsynlegur er til að tryggja rétta virkni vefsíða.
- Allur hugbúnaður sem sóttur er af Internetinu skal meðhöndlaður sem grunsamlegur og kannað hvort hann innihaldi veirur áður en hann er settur upp á nettengdri tölvu eða netþjóni.
- Óheimilt að senda upplýsingar um starfsemi fyrirtækisins eða viðskiptavini þess inn á vefsetur eða umræðuhópa á Internetinu.
- Bann er lagt við tilraunum til hvers kyns innbrota eða að rjúfa á annan hátt öryggi fyrirtækisins.

Öryggisreglurnar sem taldar eru upp hér á undan gilda um alla þjónustu-aðila Veritas.

3.5. *Öryggisreglur vegna spilli hugbúnaðar*

Allur tölvupóstur, móttekinn eða sendur er skoðaður í leit að spilli-hugbúnaði. Takmarkanir eru settar á viðhengi sem hægt er að senda eða móttaka (t.d *.exe) en starfsmaður UTD Veritas ákveður hverju sinni hvaða viðhengi um er að ræða.

Þjónustuaðilar skulu tafarlaust bregðast við tölvuvírusum eða spilli-hugbúnaði þegar hann uppgötvast með því að láta starfsmann UTD Veritas vita og varast að opna skjöl sem gætu verið sýkt.

Líta skal á allan nýjan hugbúnað sem hugsanlega smitaðan, þar á meðal hugbúnað sem fenginn er beint frá framleiðanda.

3.6. *Farsímar, lófatölvur og aðrir færanlegir geymslumiðlar*

Þjónustuaðilum er ekki leyfilegt að tengja eigin búnað við tölvukerfi Veritas nema það teljist nauðsynlegt til að leysa viðkomandi verkefni.

Dæmi um tæki sem virka sem geymslumiðlar eru: Snjallsímar, iPod, Black-berry, Palm, iPad, usb minnislyklar og usb tengdir diskar.

3.7. *Notkun þjónustuaðila á tölvubúnaði fyrirtækisins*

Notkun þjónustuaðila á tölvubúnaði Veritas og tengdra fyrirtækja, annars en þess sem þeim er sérstaklega ætlaður til vegna starfa sinna er óheimil. Þjónustuaðilar hafa möguleika á að tengjast þráðlausu neti hjá Veritas sem ætlað er gestum. Óheimilt er að tengja aðrar tölvur (einkatölvur þjónustuaðila eða gesta) við innranet Veritas.

3.8. *Aðgangsstýring kerfa*

Í þeim tilfellum þar sem þjónustuaðilum er veittur aðgangur að kerfum Veritas verða þeir að fylgja reglum um verndun lykilorða. Þjónustuaðilar skulu fylgja eftirfarandi reglum:

- Óheimilt er að lána öðrum aðgang sinn, hvort sem það eru samstarfs-menn eða starfsmenn Veritas.
- Lykilorð má ekki skrifa niður þannig að óviðkomandi gæti komist yfir lykilorðið.
- Lykilorð eiga að uppfylla þau skilyrði sem sett eru af UTD Veritas.
- Þegar farið er frá vinnustöð skal þjónustuaðili ávallt aftengjast eða læsa skjá.
- Þjónustuaðili ber fulla ábyrgð á þeim aðgangi sem honum er veittur og afleiðingum þess ef aðrir komast yfir aðgang hans.
- Aðgangsorðum skal tafarlaust breytt ef þjónustuaðili telur að aðrir viti um aðgangsorðið eða ef hann tekur eftir einhverju óvanalegu í tölvu-kerfinu.

3.9. *Öryggi gagna og hugbúnaðar*

- Óheimilt er að nota hugbúnað sem Veritas hefur ekki leyfi fyrir.
- Hugbúnaður sem ekki hefur verið samþykktur af starfsmanni UTD Veritas á ekki að setja inn á tölvur.
- Þjónustuaðilum er óheimilt að leyfa öðrum að afrita hugbúnað sem Veritas hefur þróað eða hefur leyfi til að nota og er óheimilt að gera afrit umfram þau sem kveðið er á um í viðkomandi leyfissamningum.
- Ekki má sækja eða vista óviðeigandi efni á tölvubúnaði fyrirtækisins, þar með töldum netþjónum og vinnustöðvum.
- Hvers kyns vélbúnaður og hugbúnaður sem Veritas lætur þjónustuaðilum í té er eign Veritas og getur sem slíkur sætt endur-skoðun hvenær sem er án fyrirvara.
- Þjónustuaðilum er óheimill aðgangur að tölvukerfum Veritas eða tölvutækum upplýsingum og gögnum án viðeigandi heimildar. Enn fremur er þeim óheimilt að gera ósamþykktar breytingar á búnaði, stýrikerfum, hugbúnaði eða gögnum (eyða/breyta). Þjónustuaðili þarf að geta sýnt fram á heimildargjöf þar að lútandi.

- Geymslumiðlar sem innihalda viðkvæmar upplýsingar skulu geymdir á öruggum stað. Viðkvæmar upplýsingar eru þær upplýsingar sem flokkaðar eru sem „aðgangsstýrðar“ eða „trúnaðarupplýsingar“.
- Afritun gagna af geymslumiðlum Veritas er með öllu óheimil.

3.10. *Öryggi innri neta*

Virkni innri neta er mjög mikilvæg fyrir rekstur fyrirtækisins. Allir verða að gæta þess að tengja ekki neinn búnað við netið sem gæti truflað starfsemi þess. Eftirfarandi reglur gilda fyrir alla þjónustuaðila:

- Engir aðrir en starfsmenn UTD Veritas eða þjónustuaðilar í þeirra umboði mega eiga við netbúnað fyrirtækisins.
- Ekki er leyfilegt að tengja þráðlausan búnað við innra net fyrirtækisins annan en þann sem starfsmenn UTD Veritas hafa samþykkt.
- Ekki er leyfilegt að setja upp annan netbúnað í húsnæði Veritas þó svo hann sé ekki tengdur innra neti fyrirtækisins, án samþykkis starfs-manna UTD Veritas.
- Ekki er leyfilegt að tengja annan búnað við innra net fyrirtækisins en þann sem er í eigu fyrirtækisins eða starfsmenn UTD Veritas hafa samþykkt.

3.11. *Efnislegt öryggi*

- Þjónustuaðilar skulu tryggja að allur búnaður Veritas í þeirra umsjá sé varinn gegn þjófnaði og skemmdum, hvort sem er af ásetningi, fyrir slysni eða af öðrum orsökum s.s. af völdum náttúruafla.
- Ef tölvubúnaður glatast, skemmist eða er stolið skal slíkt tilkynnt strax til starfsmanna UTD Veritas eða upplýsingaöryggisstjóra.
- Leyfi starfsmanna UTD Veritas þarf til að fjarlægja tölvubúnað úr húsnæði Veritas.
- Þjónustuaðilar skulu ekki veita óviðkomandi aðgang að lokuðum svæðum. Þjónustuaðilar skulu geyma allan aðgangsbúnað á öruggum stað.

4. Rafræn vöktun

Veritas beitir rafrænni vöktun við eftirlit t.d. með húsnæði, tölvupósti og Internettengingu. Eftirlitið er framkvæmt með gæslumyndavélum, skráningu í dagbækur tölvukerfa, eða á þann hátt sem henta þykir hverju sinni.

4.1. *Staðsetning rafrænnar vöktunar*

Rafræn vöktun og skráning á notkun er t.d. hugsanlega framkvæmd í eftirfarandi kerfum:

- Tölvupóstur.
- Notkun aðgangskorta.
- Upptökur úr gæslumyndavélum.
- Internetnotkun.
- Símanotkun.
- Inn- og útskráning á tölvubúnaði og kerfum.

4.2. *Reglur um skoðun skráa rafrænnar vöktunar*

Í flestum tilfellum er rafræn vöktun notuð til þess að hafa eftirlit með virkni búnaðar en í einstaka tilfellum er henni beitt til þess að hafa eftirlit með eignum og gæðum þjónustu.

Ef nauðsynlegt reynist að skoða notkun einstakra starfsmanna á Interneti eða tölvupósti skal sú skoðun fara fram samkvæmt reglugerð frá Persónuvernd. Starfsmönnum skal boðið að vera viðstaddir slíka skoðun nema ríkir hagsmunir Veritas liggi við t.d. ef grunur er um alvarlegt lögbrot sem gæti krafist rannsóknar lögreglu. Í slíkum tilfellum skal upplýsingaöryggisstjóri vera viðstaddur skoðun gagna.

Ekki er heimilt að skoða upptökur úr öryggismyndavélum nema fyrir liggi skriflegur rökstuðningur fyrir þörf á skoðun þeirra.