FINANTSINSPEKTSIOON

Finantsinspektsiooni soovituslik juhend

Nõuded finantsjärelevalve subjekti infoturbe korraldamisele

Soovituslik juhend on kehtestatud Finantsinspektsiooni juhatuse 04.11.2009 otsusega nr 1.1-7/52.

1. Pädevus

1.1 Finantsinspektsiooni seaduse (edaspidi nimetatud FIS) § 3 kohaselt teostab Finantsinspektsioon riiklikku finantsjärelevalvet finantssektori stabiilsuse, usaldusväärsuse ja läbipaistvuse ning toimimise efektiivsuse suurendamise, süsteemsete riskide vähendamise ning finantssektori kuritegelikel eesmärkidel ärakasutamise tõkestamisele kaasaaitamise eesmärgil, et kaitsta klientide ja investorite huve nende vahendite säilimisel ning seeläbi toetada Eesti rahasüsteemi stabiilsust.

1.2 FIS § 57 lg 1 kohaselt on Finantsinspektsioonil õigus välja anda soovitusliku iseloomuga juhendeid finantssektori tegevust reguleerivate õigusaktide selgitamiseks või finantsjärelevalve subjektide suunamiseks.

2 Eesmärk ja kohaldamisala

2.1 Infoturve on pidev protsess, mille käigus ettevõte hindab oma riske seoses infotehnoloogia kasutamisega ettevõtte tegevuses, valib meetmed riskide juhtimiseks, mõõtmiseks ja maandamiseks ning kontrollib nende meetmete toimimist.

2.2 Infoturbe peamiseks eesmärgiks on ettevõtte infotehnoloogia kasutamisega seotud riskide maandamine ettevõtte jaoks aktsepteeritavale tasemele.

2.3 Antud juhendi eesmärgiks on ühtlustada järelevalvesubjekti infoturbe protsessi korraldamist ja kirjeldada nõudeid infotehnoloogia valdkonnale, millede täitmisel saadakse kindlust infoturbe eesmärkide täitmise kohta.

2.4 Käesoleva juhendiga kehtestatakse soovituslikud ja üldise iseloomuga tegevusjuhised ja -suunised järelevalvesubjektile infoturbe protsessi korraldamiseks.

2.5 Käesolevas juhendis on soovituste ja nõuete kujundamisel aluseks võetud rahvusvaheliselt tunnustatud standardites ISO/IEC 27001 ja ISO/IEC 27002 toodud soovitused.

3 Juhendi kohaldamine

3.1 Antud juhendis on kirjeldatud Finantsinspektsiooni arvamuse kohaselt minimaalsed nõuded järelevalvesubjektide infoturbe tagamisele. Juhendi nõuete sisustamisel ja vastavate lahenduste väljatöötamisel ning rakendamisel konkreetse järelevalve subjekti poolt tuleb arvestada nii subjekti äritegevuse iseloomu, organisatsiooni ja selle toimimise komplekssust, ettevõtte mõju kogu finantssektorile tervikuna kui ka infoturbe riskide ja nende realiseerumise tagajärgede kaalukust.

3.2 Käesoleva juhendi rakendamisel tuleb arvestada õigusaktidest tulenevate nõuetega, samuti teistest Finantsinspektsiooni soovituslikest juhenditest tulenevate suunistega ja juhendit rakendava järelevalvesubjekti iseärasustega koos konkreetse subjekti sisemise infoturbe korraldusega. Õigusaktidest tulenevate erinõuete korral tuleb lähtuda õigusaktides sätestatust.

3.3 Juhendi kohaldamisel tuleb arvestada „täidan või selgitan" põhimõtet, mille kohaselt järelevalvesubjekt peab vajadusel suutma põhjendada, miks ta mõnda juhendi punkti ei rakenda või teeb seda osaliselt.

3.4 Juhendi kohaldamisel, samuti tõlgenduslike probleemide korral, tuleb lähtuda mõistlikkuse põhimõttest, arvestades käesoleva juhendi eesmärki ning toimida heas usus järelevalvesubjektilt eeldatava hoolsuskohustusega.

4 Mõisted

4.1 **Infoturve** on informatsiooni kaitse, et tagada:
- konfidentsiaalsus – informatsiooni kaitse volitamata avalikustamise eest;
- terviklus – informatsiooni kaitstus võltsimise ja volitamata muutmise eest;
- käideldavus – informatsiooni ja teenuste õigeaegne ja piisavalt süstematiseeritud kättesaadavus volitatud isikutele.

4.2 **Infoturbe meetmed** on ettevõtte poolt teostatud tegevused, protsessid ja vahendid riskide juhtimiseks, mõõtmiseks ja maandamiseks ning infoturbe intsidentide ennetamiseks, vältimiseks ja intsidentide poolt tekitatud kahjude vähendamiseks.

4.3 **Infoturbe poliitika** on dokument, mis fikseerib kirjalikult ettevõtte sihid infoturvalisuse alal ning üldreeglid nende sihtide saavutamiseks.

4.4 **Infovara** on informatsioon, andmed ja nende töötlemiseks vajalikud rakendused.

4.5 **Infovara omanik** ettevõtte töötaja, kellele on määratud vastutus infovara turvalisuse ja hoolduse eest ning kelle ülesandeks on muuhulgas andmete klassifitseerimine ja kasutajaõiguste määramine.

4.6 **Turvaintsident** on sündmus, mille tagajärjeks on (või võib olla) infoturvalisuse rikkumine.

4.7 **Tundlik informatsioon** on informatsioon, mida vastavalt pädeva organi otsusele tuleb kaitsta, sest selle avalikustamine, muutmine, hävimine või kadumine põhjustaksid olulist kahju.

4.8 **Turvaala** on ettevõtte ruumides asuv ala, kuhu paigutatakse kriitilised infrastruktuuri komponendid ja mille kaitseks on rakendatud eraldi turvameetmed.

4.9 **Järelevalve subjekt** on käesoleva juhendi tähenduses FIS § 2 lg 1 alusel finantsjärelevalve subjektina käsitletav isik, sealhulgas välisriigi krediidiasutuse, kindlustusandja, investeerimisühingu ja fondivalitseja filiaal õigusaktides sätestatud ulatuses ja mahus. Järelevalve subjektina käesoleva juhendi tähenduses ei käsitleta kindlustustegevuse seaduse §-s 130 lõikes 2 p 1 nimetatud kindlustusmaaklerit.

5 Infoturbe koht

5.1 Infoturbega seotud küsimused peavad olema järelevalve subjekti riskijuhtimise lahutamatuks osaks.

5.2 Infoturbega seotud tegevused peavad viima selleni, et järelevalvesubjekti infoturbealased riskid on kaardistatud ja infoturbe intsidentide tekkimise ennetamiseks on rakendatud sobivad meetmed ning infoturbe intsidentide tekkimisel rakendatakse eeldefineeritud protseduurid ja tegevuskavad, mis tagavad intsidendi kiire lahenduse kahju minimeerimiseks.

6 Infoturbe poliitika

6.1 Järelevalve subjekti üldised infoturbe põhimõtted tuleb fikseerida infoturbe poliitikas. Juhatus peab seadma poliitikaga kindla sihi, näitama toetust ja abi infoturbe tagamisele organisatsioonis.

6.2 Infoturvalisuse tagamine on ettevõtte riskijuhtimise osa ja infoturbe poliitika peab olema kooskõlas ettevõtte riskihindamise tulemustega ning vastama ettevõtte infoturbe tasemele.

6.3 Infoturbe poliitikas peab olema defineeritud infoturbe mõiste ja kirjeldatud meetmed, millega tagatakse infoturve, infoturbe eest vastutavad isikud ning infoturbe rakendamist toetavad tegevuskavad, standardid, protseduurid ja juhendid.

6.4 Järelevalve subjekti töötajad peavad olema teadlikud organisatsioonis kehtivast infoturbe poliitikast ja sellest tulenevatest alamdokumentidest ning töötajate rollist ja vastutusest

infoturbe tagamisel. Infoturbe poliitika olulise muudatuse korral tuleb sellest teavitada organisatsiooni töötajaid, samuti peab uute töötajate värbamisel neile tutvustama kehtivat infoturbe poliitikat.

6.5 Lähtuvalt järelevalve subjekti tegevusvaldkonnast, äri- ja IT strateegiast ning riskitaluvusest tuleb kehtestada infoturbe poliitika dokumendi ülevaatamise sagedus. Samuti peab olema tagatud, et infoturbe poliitika vaadatakse üle ning vajadusel täiendatakse iga suurema muudatuse korral järelevalvesubjekti äritegevuses või infotehnoloogia korralduses.

7 Infoturbe organisatsioon

7.1 Üldine vastutus infoturbe tagamise eest on ettevõtte juhatusel. Ettevõttes tuleb määrata eraldi infoturbe eest vastutav isik, olenevalt organisatsiooni suurusest ja tegevuse komplekssusest võiks kaaluda eraldi ametikoha loomist. On soovitav, et vastutus infoturbe koordineerimise eest oleks määratud ühele juhtkonna liikmele.

7.2 Infoturbe eest vastutava isiku kohustuseks peab olema ettevõtte infoturbe korralduse vastavuse tagamine infoturbe poliitikale, sisemistele kordadele ning välistele nõuetele. Üheks põhiülesandeks peab ettevõtte infoturbe eest vastutaval isikul olema teiste organisatsiooni töötajate tegevuste koordineerimine turvalisuse tagamiseks.

7.3 Järelevalve subjekti ärivaldkonna kaasamiseks infoturbega seotud küsimuste lahendamisesse on soovitatav moodustada infoturbe juhtrühm (*steering commitee*), kuhu peaksid kuuluma kõigi oluliste äriüksuste või funktsioonide juhid ning infoturbe juht.

7.4 Organisatsiooni infoturbe poliitikas määratletud konfidentsiaalsusnõuded, turvarollid ja vastutus peavad olema iga töötaja jaoks fikseeritud. Infoturbe tagamine oma tööülesannete täitmisel peab olema organisatsiooni iga töötaja vastutus ja see peab selgelt väljenduma nii organisatsiooni kultuuris kui ka töötajatega sõlmitavates kokkulepetes. Töötajad peavad olema teadlikud oma kohustustest ja vastutustest ettevõtte infoturbe tagamisel.

7.5 Järelevalve subjekt peab hindama väliste teenusepakkujate kasutamisest tulenevaid riske, muuhulgas riske andmeturbele. Sellist hindamist tuleb teha nii välise teenusepakkuja valikul, teenuse edasiandmise lepingu sõlmimisel kui ka vastavate teenusetasemetes kokkuleppimisel. Vastavalt edasi antud teenuse olemusele tuleb kindlaks määrata, millistele turvalisuse nõuetele peab teenuse osutaja vastama. Ettevõttes peab olema kehtestatud kontrollimehhanism, mis tagaks välise teenusepakkuja infoturbe võimekuse hindamise. Täpsemad nõuded tegevuse edasiandmise kohta on kirjeldatud 25.10.2006 Finantsinspektsiooni juhatuse otsusega nr 1.1-7/84 kehtestatud soovituslikus juhendis „Nõuded finantsjärelevalve subjekti poolt tegevuse edasiandmisele“.

8 Inimressursi turve

8.1 Ettevõttes peavad olema kehtestatud mehhanismid vastutavatele ametikohtadele võetavate töötajate (näiteks ettevõtte infosüsteemides eriõigusi omavad töötajad) tausta kontrollimiseks. Arvesse tuleb võtta lisaks erialasele kompetentsusele ka ettevõtte tegevusvaldkonda ja vajadust töötada tundliku informatsiooniga.

8.2 Enne kasutajatele infovarale juurdepääsu andmist peab olema tagatud nende informeeritus nii organisatsiooni poliitika ja protseduuride osas (kaasa arvatud turvanõuded ja muud talitlusmehhanismid) kui ka infotehnoloogia vahendite otstarbekohase kasutamise vallas. Turvateadlikkuse tõstmiseks on soovitatav ettevõttes korraldada regulaarselt koolitusi, mis hõlmaksid kõiki töötajaid (kaasa arvatud juhtkond) ning tutvustaksid eeskätt ettevõtte infoturbepoliitikat, infoturbe tähtsuse põhjuseid, sellega seotud kohustusi ning protseduure, turvanõudeid, turvaintsidentidest teavitamist ning nende toimet.

8.3 Täiendava infoturbe meetmena on soovitav ettevõtte töötajatega sõlmitavates töölepingutes sätestada muuhulgas konfidentsiaalse informatsiooni hoidmise kohustus ja selle kohustuse rikkumisega kaasnev vastutus ka peale töötaja lahkumist ettevõttest.

8.4 Töötajate õigused, kohustused ja vastutus peavad olema määratletud infoturbe juhendites ja muudes asjakohastes siseregulatsioonides.

9 Füüsiline ja keskkonna turve

9.1 Järelevalve subjektil tuleb kaardistada ettevõtte piirkonnad, mida infoturbe seisukohast tuleb kaitsta ja kuhu tohivad siseneda vaid selleks volitatud töötajad. Kriitilisi või tundlikke talitlusfunktsioone toetavad infotehnoloogiavahendid tuleb paigutada piiratud juurdepääsuga turvaaladele ning neid tuleb füüsiliselt kaitsta volitamata pöördumiste, kahjustuste, turvaohtude (nt. tulekahju) ja keskkonnariskide eest.

9.2 Piiratud juurdepääsuga turvaalade kaitseks tuleb kasutada füüsilisi ja loogilisi juurdepääsukontrolle selliselt, et ainult volitatud isikud saavad piirkonda sissepääsu. Samuti tuleb rakendada mehhanism, mis tagaks, et kõik sellisesse piirkonda sisenemised fikseeritaks.

9.3 Turvameetmete valimisel turvaalade kaitsmiseks on soovitav võtta aluseks mõne sõltumatu ja tunnustatud organisatsiooni poolt kirjeldatud standardid. Meetmete valimisega tuleb alustada juba turvalise piirkonna asukoha valikul ja meetmete rakendamisega selle väljaehitamisel ning sisustamisel. Serveriruumi teenuse edasiandmisel peaksid teenusepakkuja ja pakutava lahenduse valikul kehtima samad standardid.

9.4 Turvaliste piirkondade puhul tuleb vältida nende tähistamist üldarusaadavalt ja kandmist viitadele. Turvaliste piirkondade planeerimisel tuleks vältida nende rajamist akendega ruumi.

9.5 Vältida tuleb side- ja elektrikaablite vigastamise võimalust füüsiliselt ja ettevaatamatuse tõttu. Selleks on soovitav kasutada kaabelduse jaoks eraldi kandekonstruktsiooni ja üldkäidavates kohtades see varjata sobivate materjalidega. Side- ja elektrikaablite

ühenduskohtades tuleb kasutada vastavat märgistust, mis võimaldab probleemi tekkimisel võimalikult kiiresti tuvastada selle põhjuse.

10 Side ja operatsioonide turve

10.1 Piiratud juurdepääsuga turvaalasid tuleb pidevalt monitoorida võimalike kahjustuste ennetamiseks ja kahjustuste korral nende kiireks avastamiseks.

10.2 Seire korraldamiseks on vajalik infosüsteemis läbiviidavate toimingute kontrolljälg. Infosüsteemi osade sobiv seiretase tuleb määrata riskihinnangute alusel. Kontrolljäljed ehk logid tuleb teha ettevõttele tähtsa informatsiooni kohta arvestades vähemalt järgmisi võimalikke sündmusi:

- kasutajate sisenemine süsteemi;
- informatsiooni vaatamine;
- päringute tegemine;
- süsteemide ja aplikatsioonide poole pöördumine;
- andmebaasi muudatused ja tehingud;
- katsed saada ligi tundlikule informatsioonile;
- süsteemide kasutus spetsiaalsete (laiendatud) kasutusõigustega;
- autoriseerimata toimingud infosüsteemis.

10.3 Volitamata toimingute õigeaegseks avastamiseks ning rakendatud juurdepääsukontrolli meetmete tõhususe hindamiseks peab olema rakendatud sobiv süsteemipääsu ja –kasutuse seire. Volitamata toiminguks on igal juhul selline, millega rikutakse õigusaktide nõudeid või mille eesmärgiks või sisuks on finantsjärelevalve teostaja või uurimisasutuse haldusakti või toimingu ebakohane täitmine või täitmata jätmine, sh informatsiooni tervikluse või käideldavuse rikkumine võrreldes ettevõtte poolt akti saamisele või toimingu tegemisele eelneva ajaga. Finantsjärelevalveasutuse poolt vastava nõude saamisel järelevalve subjekt detailselt põhjendab eelmises lauses kirjeldatud volitamata toimingut.

10.4 Logide läbivaatust tuleb teostada juhul, kui on põhjendatud kahtlus organisatsiooni töötaja või kliendi tehingute õiguspärasuses ja samuti juhul, kui on reaalne ettevõtte informatsiooni käideldavuse, tervikluse või konfidentsiaalsuse rikkumise oht.

10.5 Salvestatud logide haldamiseks peavad olema kehtestatud protseduurid ja välja töötatud meetmed, mis kaitseksid logide käideldavust, terviklust ja konfidentsiaalsust. Logifailide andmekandjaid on soovitav hoida turvalises piirkonnas ja eraldi logitavast infotöötluskeskkonnast.

10.6 Ettevõttes peavad olema dokumenteeritud ja juurutatud varukoopiate tegemise protseduurid. Varukoopiaid tuleb teha regulaarselt ning hoida neid turvalises piirkonnas, mis välistab volitamata juurdepääsu ja tagab koopiate füüsilise kaitse. Ühte eksemplari varukoopiatest tuleb regulaarselt ning turvaliselt ladustada varukoopiate tegemise hoonest geograafiliselt eraldi asetsevas asukohas. Varukoopiate kasutuskõlblikkust ning täielikkust tuleb regulaarselt kontrollida.
Varukoopiate tegemise protseduur peab käsitlema vähemalt järgmisi teemasid:

- informatsioon, millest on vaja teha varukoopia;
- varukoopiate tegemise ulatus ja sagedus;
- vastutus varukoopiate tegemise eest;
- varukoopiate säilitamise aeg;
- varukoopiast andmete taastamine.

10.7 Järelevalvesubjektil peavad olema kehtestatud reeglid sätestamaks, millist teavet ja millisel teel ettevõte välise osapoolega vahetab ning kuidas seda teavet kaitstakse. Ohu realiseerumise korral peab olema võimalik rakendada alternatiivseid infoedastamise võimalusi.

10.8 Ettevõttes tuleb tagada konfidentsiaalsete andmete kaitse nende edastamisel avaliku võrgu kaudu. Konfidentsiaalsete andmete edastamisel üle avaliku võrgu tuleb välistada andmete avalikuks tulemise võimalus kolmandatele isikutele. Suurema ohu korral tuleb kaaluda kogu avalikus võrgus toimuva infovahetuse krüpteerimist. Võrguturbe meetmed tuleb kehtestada nii võrku pääsemise, võrgus kasutatavate teenuste kui ka võrgus teostatud toimingute kohta.

10.9 Ründetarkvara ja viiruste õigeaegseks avastamiseks ja tõkestamiseks peavad olema rakendatud vajalikud meetmed ning määratud vastutus. Lisaks tuleb tagada kasutajate viivitamatu teavitamine ründetarkvara ja viirustega kaasnevate ohtude osas siis, kui adekvaatsetest infoallikatest pärineva teabe põhjal on ründetarkvara ja/või viiruste levikust tulenev reaalne oht ettevõttele suurenenud.

10.10 Järelevalve subjektil peavad olema kehtestatud meetmed teisaldatavate infotehnoloogiliste seadmete (näiteks sülearvutid) ja teisaldatava meedia (näiteks mälupulgad) kaitseks. Suurema ohu korral meediale endale tuleb sellel sisalduvad andmed infotehnoloogiliste meetmetega kaitsta näiteks andmete krüpteerimise teel.

11 Pääsu reguleerimine

11.1 Ettevõttes peavad pääsuõiguste jaotuse reguleerimiseks olema kehtestatud poliitikad või protseduurid, mis hõlmavad pääsu elutsükli kõiki faase, sh kasutajate esialgset registreerimist, pääsuõiguste muutmist ja nende kasutajate lõplikku väljaregistreerimist ehk kasutajaõiguste peatamist või katkestamist, kes infoteenuseid enam ei vaja. Pääsuõiguste poliitikad või protseduurid peavad määratlema kõikvõimalikud juurdepääsukohad, sh töökoha arvutile ligipääsu, andmesidevõrku pääsu, operatsioonisüsteemidele ligipääsu, rakendustele ja andmebaasidele ligipääsu, mobiilse- ja kaugjuurdepääsu infovaradele, ajutiste töötajate ja väliste kasutajate ligipääsu infosüsteemile. Pääsuõigused ja muu töökorraldus peavad olema reguleeritud selliselt, et infovara kasutaja on ettevõtte poolt piisava kindlusega tuvastatav. Infovara kasutajaks olnud ettevõtte ja tema kontserni äriühingu töötaja ning juhtorgani liige peab olema individuaalselt (ja mitte kollektiivselt) tuvastatav iga muudatuse või kustutamise osas.

11.2 Järelevalve subjektil peavad olema kehtestatud reeglid salasõnade valikuks ja halduseks. Infosüsteemis antud kasutajaõigustele vastavad salasõnad peavad olema vähemalt sellise keerukusega, et nende ära arvamine proovimise teel oleks suure tõenäosusega välistatud.

11.3 Salasõnade halduse kord peab olema kooskõlastatud organisatsiooni infovara omanikega, see peab olema kõigile infovarale juurdepääsu omavatele töötajatele teada ning peab sisaldama informatsiooni vähemalt järgmise kohta – salasõnade loomise ja teavitamise protseduur, salasõna muutmise sagedus ja tingimused, salasõnade hoidmine, kasutajate vastutus ning eriõigustega kasutajate salasõnade haldamise reeglid.

11.4 Kasutajaid tuleb teavitada nende kohustusest salasõnade turvalisel kasutamisel. Kasutaja salasõnaga infosüsteemis tehtud toimingute eest on vastutav kasutaja, kellele vastava salasõnaga ligipääs infosüsteemile antud on.

11.5 Juurdepääs andmetele ja informatsioonile peab olema piiratud isikutega, kellele on seda oma tööülesannete täitmiseks vaja. Juurdepääsuõiguste andmine peab olema kooskõlastatud infovara omanikuga. Antud pääsuõigused peavad olema dokumenteeritud ja põhinema infovara omaniku tahtel.

11.6 Järelevalve subjektil tuleb kehtestada ja rakendada ligipääsuõiguste kontrolli protseduur. Dokumenteeritud ja reaalselt antud pääsuõiguste vastavust tuleb regulaarselt kontrollida, samuti tuleb regulaarselt hinnata kasutajale antud õiguste vastavust tema vajadustega. Kontrolli käigus tuvastatud ligipääsuõigused, millel tegelik kasutaja puudub, tuleb eemaldada.

11.7 Erilist tähelepanu tuleb pöörata ligipääsuõiguste õigeaegsele sulgemisele juhul, kui töötaja lahkub ettevõttest. Töötaja usalduse kaotuse puhul tuleb töötaja ligipääsuõigused infosüsteemides sulgeda enne kui töötajale tehakse ametlikult teatavaks tema töösuhte lõppemine. Töötaja pikema eemalviibimise korral tuleb kaaluda töötajale antud pääsuõiguste peatamist eemalviibimise ajaks.

11.8 Kõik infovarade kasutajad tuleb identifitseerida ja autoriseerida. Vastavalt infovarade tundlikkusele tuleb kehtestada kasutajate identifitseerimise ja autoriseerimise tase ning vastavad reeglid.

11.9 Väljastpoolt ettevõtte sisevõrku infosüsteemi teenuste kasutamist tuleb erilise hoolega jälgida. Enne teenuse avamist ja vastavate ligipääsuõiguste andmist peab olema tagatud välise kasutaja identiteet ja autentsus konkreetse teenuse kasutamiseks ning vastavate toimingute tegemiseks. Vastavalt teenuse iseloomule tuleb kaaluda sellise teenuse kasutajate kahese identifitseerimise ja autentimise lahendust (*two factor authentication*).

12 Infosüsteemide turve

12.1 Infosüsteemide turvalisuse vajadus ja vastavad kontrollid peavad olema määratud infovara omaniku poolt või temaga koostöös. Infovara omanik tagab finantsjärelevalvet teostava asutuse ja uurimisasutuse soovitavate andmete tervikluse ja käideldavuse.

12.2 Ettevõtte infosüsteemide arendamisel ja täiendamisel ning muutmisel peab olema tagatud, et infosüsteemid töötlevad infot ettenähtud korras. Andmekvaliteedi tagamist peavad toetama kontrollid nii andmete sisestamisel kui väljundi kasutamisel.

12.3 Infosüsteemi muudatuste tagajärjel tekkida võivate õigusaktide nõuete rikkumise tõenäosuse vähendamiseks tuleb kavandatava muudatuse eesmärki arvestades tagada muudatuste teostamise õiguspärasus.

12.4 Vastavalt vajadusele ja informatsiooni tundlikkusele eeskätt konfidentsiaalsuse ja tervikluse tagamiseks tuleb informatsiooni kaitseks rakenda krüpteerimist. Ettevõttes tuleb kehtestada reeglid krüpteerimise kasutamiseks. Reeglid peavad sätestama, millisel juhul on andmete krüpteerimine kohustuslik. Samuti peab olema kokku lepitud kasutatav krüptograafiline algoritm, minimaalsed krüptovõtme pikkused ja see, kuidas krüptograafilisi võtmeid hallatakse.

12.5 Tarkvara tehnoloogiast tulenevate nõrkuste kaitseks peavad ettevõttes olema kehtestatud reeglid tarkvarauuenduste väljaandmise jälgimiseks ja nende testimiseks ning rakendamiseks. Tarkvarauuenduste halduse vastutus peab olema määratud igale eraldiseisvale tarkvaralisele süsteemile.

12.6 Ettevõte määratleb ja kehtestab infovara säilitamise aja arvestades õigusaktide nõudeid, aegumistähtaegu ja finantsjärelevalve asutuse võimalikku huvi info suhtes.

12.7 Ettevõte tagab, et (loodud ja/või töödeldud) ametialane info salvestatakse esimesel võimalusel ka ettevõtte valduses või kasutuses olevas riistvaras, kui ettevõtte töötaja ja juhtorgani liige viidatud ametialast infot loob või töötleb ettevõtte valduses või kasutuses mitteolevas riistvaras (isiklik arvuti, isiklik postkast teenusepakkuja juures, vmt), kui õigusakt ei nõua kohest salvestamist.

13 Infoturbeintsidentide haldus

13.1 Turbe rikkumisel on vaja tagada sellest viivitamatu teavitamine, registreerimine, intsidendi verifitseerimine selleks pädeva töötaja poolt ja meetmete rakendamine.

13.2 Lisaks Finantsinspektsiooni 22.09.2004 juhatuse otsusega nr 44-4 kehtestatud soovitusliku juhendi „Nõuded infotehnoloogia ala korraldamiseks“ punktis 18. Probleemide ja intsidentide haldus toodud nõuetele tuleb infoturbe intsidendi lahendamisel pöörata tähelepanu intsidendi lahendamise käigus saadud informatsiooni säilitamisele selliselt, et hilisemal uurimisel oleks võimalik täpselt tuvastada, mis juhtus ja saada kinnitus selle kohta, et informatsiooni järelduste tegemiseks ei ole intsidendi ilmnemisest kuni selle lahendamiseni muudetud.

13.3 Ettevõtte sisesed protseduurireeglid peavad tagama, et igale tuvastatud ja raporteeritud turvaintsidendile määratakse vastutaja, kelle peamiseks eesmärgiks on intsidendi lahendamise koordineerimine intsidendi vältel. Protseduurireeglid peavad muuhulgas sisaldama intsidendi potentsiaalse eskaleerumise kirjeldust. Nõuded talitluspidevuse intsidentide lahendamiseks vastavalt ettevõtte talitluspidevuse plaanile on kirjeldatud Finantsinspektsiooni 06.12.2006 juhatuse otsusega nr 96 kehtestatud soovituslikus juhendis „Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamisele“.

13.4 Toimunud infoturbe intsidente tuleb analüüsida, et välja selgitada nende põhjused, tuvastada puudused ja välja töötada meetmed nende puuduste likvideerimiseks ning seeläbi vältida sarnaste intsidentide kordumist tulevikus. Samuti aitab intsidentide analüüsimine välja selgitada, milliseid teadmisi on vaja arendada organisatsiooni töötajates ja ettevõtte klientides vältimaks sarnaste intsidentide tekkimist ja teadvustada ettevõtte siseselt, kuidas intsidentide lahendamist tulevikus paremini korraldada.

14 Infoturbe auditite vajaduse hindamine ja auditite planeerimine

14.1 Lisaks Finantsinspektsiooni 22.09.2004 juhatuse otsusega nr 44-4 kehtestatud soovitusliku juhendi „Nõuded infotehnoloogia ala korraldamiseks“ punktile 21. Seire ja hindamine tuleb ettevõttes pöörata tähelepanu infoturbe auditeerimisele. Ettevõtte infotehnoloogia ja infoturbe tegevuste planeerimisel tuleb tagada järelevalveliste tegevuste tõhus toetus finantsjärelevalvet teostavale asutusele. Ettevõtte siseauditi plaani koostamisel peab arvestama muuhulgas infoturbe auditi alaste tegevustega.

14.2 Infoturbe nõuetele vastavust tuleb ettevõttes pidevalt jälgida ja mõõta, vajadusel tuleb konsulteerida asjatundjatega ja rakendada sõltumatu kontrollifunktsioon nõuete täitmise hindamiseks.

14.3 Infoturbe auditite vajaduse peab välja selgitama riskianalüüsi käigus. Riskianalüüsi tulemusena ilmnevad kõige kriitilisemad valdkonnad, mille osas auditi läbiviimist kaaluda tuleb. Infoturbe auditi eesmärgiks peab olema sõltumatu hinnangu andmine ettevõtte vastavusele siseste ja väliste infoturbe alaste nõuetega.

14.4 Infoturbe auditi planeerimisel tuleb paika panna auditi funktsioon, protseduur, auditi plaan ja täpsemad audiitori tööülesanded ning kohustused organisatsiooni töötajatele seoses auditi läbiviimisega.

14.5 Infoturbe auditi vajaduse tuvastamisel ja auditi planeerimisel tuleb vastava oskusteabe puudumisel kaaluda IT auditite läbiviimise teenuse edasiandmist. Auditi läbiviimise edasiandmisel teenusena tuleb hinnata teenusepakkuja kompetentsi ning kogemust sarnaste auditite läbiviimisel ja erilist rõhku tuleb pöörata teenuse osutaja kohustusele hoida ja kaitsta teenuse osutamise käigus saadud konfidentsiaalset informatsiooni. Täpsemad nõuded tegevuse edasiandmise kohta on kirjeldatud 25.10.2006 Finantsinspektsiooni juhatuse otsusega nr 1.1-7/84 kehtestatud soovituslikus juhendis „Nõuded finantsjärelevalve subjekti poolt tegevuse edasiandmisele“.

14.6 Auditi tähelepanekud ja märkused tuleb võtta arvesse ettevõtte infoturbe juhtimisel ja planeerimisel. Kui auditi käigus avastatakse tõsisemaid puudusi ettevõtte infoturbega seonduvalt, tuleb peale puuduste kõrvaldamist teostada järelaudit.

14.7 Võimalike nõrkuste väljaselgitamiseks kriitiliste infosüsteemide juures tuleb alternatiivina põhjalikule auditile kaaluda ründetestide (*penetration testing*) läbiviimist. Ründetestide läbiviimisel peab olema tagatud, et ettevõtte normaalne töö ei saaks häiritud ega ettevõtte tööalane informatsioon kahjustatud.

15 Rakendamine

15.1 Käesolev juhend jõustub alates 04.05.2010. a.

15.2 Käesoleva juhendi vastuvõtmisega ja jõustumisega muudetakse Finantsinspektsiooni soovitusliku juhendi „Nõuded infotehnoloogia ala korraldamiseks“ punkti 16 ja punkti 19.