FINANTSINSPEKTSIOON

NÕUDED INFOTEHNOLOOGIA ALA KORRALDAMISEKS

Soovituslik juhend on kehtestatud Finantsinspektsiooni juhatuse 22.09.2004 otsusega nr. 44-4 Finantsinspektsiooni seaduse § 57 lg 1 alusel.

I osa Üldsätted ja mõisted

1. Soovitusliku juhendi eesmärk ja kohaldamine

1.1. Finantssektori ettevõtete tegevus sõltub olulisel määral infotehnoloogiast ("**IT**"). Juhendi eesmärgiks on kehtestada miinimumnõuded finantssektori ettevõtetes infotehnoloogiaalaseks töökorralduseks, et suurendada finantssektori efektiivsust ja vähendada süsteemseid ning operatsioonilisi riske.

1.2. Käesolev juhend reguleerib infotehnoloogiaalast töökorraldust Finantsinspektsiooni seaduse §2 lõikes 1 toodud finantsjärelevalve subjektides.

Juhendis esitatud juhised on mõeldud järgimiseks kooskõlas õigusaktides kehtestatud nõuetega.

1.3. Käesoleva juhendi koostamisel on võetud aluseks rahvusvaheliselt üldtunnustatud infotehnoloogia auditi ja juhtimise standardis COBIT (*Control Objectives for information and Related Technology*) ning selle lühivariandis COBIT *Quickstart* toodud juhtimiseesmärgid. COBIT-i juhtimiseesmärke on täiendatud ja täpsustatud infotehnoloogiat käsitlevates standardites (BS:7799, EVS- ISO/IEC 2382) sisalduvate nõuete ja definitsioonidega.

1.4. Finantssektori ettevõtte infotehnoloogia juhtimissüsteem või raamstruktuur peab olema loodud selliselt, et see tagaks sobiva toe äriprotsessidele. Ettevõtte infosüsteemid peavad vastama äritegevusest tulenevatele käideldavuse, terviklikkuse ja konfidentsiaalsuse nõuetele. Käesoleva juhendi rakendamine ettevõtetes sõltub eelkõige ettevõtete suurusest, protsesside keerukusest, töötajate arvust või kasutatavast tehnoloogiast.

2. Juhendis kasutatavad mõisted

2.1. Andmed – informatsiooni taastõlgendatav esitus formaliseeritud kujul, mis sobib edastuseks, tõlgenduseks või töötluseks.

2.2. Andmeelement – andmeüksus, mis teatud kontekstis loetakse jagamatuks.

2.3. Andmemudel – andmete korralduse kirjeldus ettevõtte infostruktuuri peegeldaval viisil.

2.4. Informatsioon – teadmus, mis puudutab objekte, näiteks fakte, sündmusi, asju, protsesse või ideid, sealhulgas mõisteid, ja millel on teatavas kontekstis eritähendus.

2.5. Infosüsteem – informatsiooni andev ja jaotav infotöötlussüsteem koos juurdekuuluvate õiguslike lahenduste ja organisatsiooniliste ressurssidega, sealhulgas inim-, tehniliste ja rahaliste ressurssidega.

2.6. Infoturve – informatsiooni kaitse, et tagada:

- konfidentsiaalsus – informatsiooni kaitse volitamata avalikustamise eest;
- terviklus – informatsiooni kaitstus võltsimise ja volitamata muutmise eest;
- käideldavus – informatsiooni ja teenuste õigeaegne kättesaadavus volitatud isikutele.

2.7. Infovara – informatsioon, andmed ja nende töötlemiseks vajalikud rakendused.

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

2.9. Tundlik informatsioon – informatsioon, mida vastavalt pädeva võimu otsusele tuleb kaitsta, sest selle avalikustamine, muutmine, hävimine või kadumine põhjustaksid kellelegi või millelegi olulist kahju.

2.10. Turvaintsident – sündmus, mille tagajärjeks on (või võib olla) infoturvalisuse rikkumine.

II osa Planeerimine ja organiseerimine

3. Strateegia

3.1. Ettevõtte infotehnoloogiaalase tegevuse aluseks peab olema juhtkonna poolt kinnitatud ettevõtte ärieesmärkidest ja -strateegiast lähtuv strateegia (IT strateegia). IT strateegia loomisel tuleb hinnata, millist infotehnoloogilist tuge on vaja ettevõtte ärieesmärkide saavutamiseks ning kas olemasolevad IT lahendused võimaldavad saavutada soovitud ärilist tulemust. Lähtuvalt IT strateegiast tuleb koostada arenguplaanid ning määratleda IT projektide prioriteedid ja investeeringud.

3.2. IT strateegiat tuleb regulaarselt kaasajastada ja täiendada vastavalt muudatustele ettevõtte äristrateegias või infotehnoloogia arengusuundades. IT strateegilise planeerimise protsessis peavad osalema nii ettevõtte äri- kui IT vastutusala juhid.

4. Infoarhitektuur

4.1. Ettevõttel peavad olema üldised reeglid infovarade omanike määramiseks ja infovarade klassifitseerimiseks turvaklassidesse ning kõikidele infovaradele peavad olema nimetatud omanikud. Tulenevalt andmete turvaklassist peavad olema kehtestatud neile vastavad juurdepääsupiirangud.

4.2. Ettevõttes peavad olema kehtestatud, juurutatud ja rakendatud turvatasemed igale infovarade turvaklassile. Turvatasemed peavad sätestama regulaarselt ülevaadatavad ning vajadusel täiendatavad miinimumnõuded turvalisuse ja kontrollialastele meetmetele.

4.3. Juhtkond peab kehtestama infovarade turvaklasside määramise protseduurid. Infovara klassifitseerimise ja juurdepääsupiirangute kehtestamise eest vastutab vastava infovara omanik.

5. IT organisatsioon

5.1. Äriprotsessidele vajaliku infotehnoloogilise toe osutamiseks peab ettevõttes olema suuruselt ja kompetentsidelt sobiv IT organisatsioon. Kui infotehnoloogia-alane oskusteave ostetakse ettevõttest väljastpoolt, tuleb määrata valdkonnad, kus võib kasutada väljasttellimist ning kelle poolt ja kuidas väljast tellitud teenuseid hallatakse.

5.2. IT personali värbamiseks peavad ettevõttes olema kehtestatud asjakohased protseduurid, mis võimaldavad hinnata isiku sobivust ametikohale. Arvesse tuleb võtta lisaks erialasele kompetentsusele ka ettevõtte tegutsemissfääri ja vajadust töötada tundliku informatsiooniga.

5.3. Ettevõtte IT organisatsioonil peavad olema selgelt määratletud struktuur ja ülesanded. Tuleb tagada vajalike ressursside olemasolu nende kohustuste täitmiseks. Töötajatel peavad olema selgelt määratletud nõutavad oskused, õigused, vastutus ja kohustused ning neid tuleb regulaarselt üle vaadata.

5.4. Ettevõttes peab olema rakendatud infotehnoloogia arenduse, hooldamise, kasutamise ja kontrolli funktsioonide lahusus. Juhul kui töökohustuste lahususe sisse viimine ei ole võimalik, tuleb rakendada riskide maandamiseks muid täiendavaid kontrolle.

6. IT investeeringute juhtimine

6.1. Infotehnoloogiasse tehtavate kulutuste ärieesmärkidele vastavaks ja optimaalseks juhtimiseks peab IT-investeeringute juhtimine toimuma läbi perioodiliselt toimuva eelarvestamise protsessi.

6.2. Juhtkond peab vähemalt üks kord aastas analüüsima ettevõtte IT olukorda. Soovitav on regulaarselt üle vaadata IT ressursside otstarbekas kasutamine äristrateegiate toetuseks ning kinnitada järgmise perioodi eelarve.

7. Vastavus välisnõuetele

7.1. Ettevõtte juhtkond peab tagama ettevõtte IT korraldamise vastavuse regulaarse hindamise välistele nõuetele (seadused, regulatsioonid, jmt) ning nende mõjudega arvestamise. Vajadusel tuleb rakendada meetmeid IT korralduse vastavusse viimiseks väliste nõuetega.

8. Riskihaldus

8.1. Ettevõtte juhtkond peab tagama infotehnoloogiaga seotud riskide haldamise protsessi toimimise, mis määratleks riskide juhtimise metoodika, aruandekohustuse ja kontrollmehhanismid. Tagada tuleb riskihinnangute regulaarne uuendamine ning riskide haldamise protsessi järjepidevus.

8.2. Kulutused IT turvalisusele ja IT teenustele peaksid olema põhjendatud riski- ja tasuvuse hinnangutega. Riskianalüüsi käigus tuleb selgitada välja võimalikud ohud, nõrkused, hinnata ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid, valida sobivad meetmed ohtude realiseerumise mõju vähendamiseks, hinnata nende tasuvust ja otsustada aktsepteeritava jääkriski suurus.

8.3. Riskide hindamine peab kaasnema iga olulise muudatusega infosüsteemides või protsessides. Infotehnoloogilise süsteemi muutuste planeerimisel tuleb kindlaks teha, kas ja kuidas muudatus mõjutab süsteemi ja protsessi turvalisust ning vähendada igakülgselt muudatusega kaasnevate riskide mõju.

9. Projektide haldus

9.1. Iga olulisem arendustegevuse projekt infotehnoloogia valdkonnas peab omama täpselt määratletud ja mõõdetavat eesmärki ning täpset algust ja lõppu omavat tähtaega. Infosüsteemi arendamine peab lähtuma ettevõtte vajadustest ning otsuse projektide käivitamise kohta peab tegema juhtkond tuginedes kinnitatud IT strateegiale.

9.2. Iga projekti elluviimiseks tuleb moodustada projektorganisatsioon. Pidevalt tuleb jälgida projekti käiku, eelarvet ja ajakava.

III osa Hankimine ja rakendamine

10. Süsteemiarendus

10.1. Ärinõuete täitmiseks sobivate lahenduste loomiseks peab toimuma eelnev kasutajanõuete väljaselgitamine ja alternatiivsete lahenduste hindamine. Juhtkonna otsus arendusprojekti alustamise ja alternatiivse lahenduse valiku osas tuleb teha tuginedes teostatavusanalüüsile, milles näidatakse ära projekti tehniline, operatsiooniline ning majanduslik põhjendatus.

10.2. Rakendustarkvara arendamisel tuleb tagada arendus-, testimis- ja tootmiskeskkonna lahusus.

10.3. Lahenduse väljatöötamisel on vaja spetsifitseerida lahenduse funktsionaalsed ja ekspluatatsioonilised nõuded, sealhulgas hooldatavus, jõudlus, töökindlus, seire, turvalisus ja ühilduvus olemasolevate süsteemidega. Selgelt tuleb määratleda testimisstandardid ning süsteemi vastuvõtukriteeriumid. Süsteeminõuded, standardid, vastuvõtukriteeriumid ning intellektuaalse omandi õigused tuleb fikseerida ka arendustööde tellimisel välistelt teenusepakkujatelt.

11. Protseduuride haldus

11.1. Infosüsteemi halduseks ja kasutamiseks peavad olema kehtestatud dokumenteeritud tööjuhised ning protseduurid. Infosüsteemis muudatuste tegemisel tuleb üle vaadata ka vastavad protseduurid ning teavitada kasutajaid teostatud muudatustest.

12. Muudatuste haldus

12.1. Infosüsteemi muudatuste tagajärjel tekkida võivate katkestuste ja vigade tõenäosuse vähendamiseks tuleb tagada muudatuste teostamise korrektsus ja kontrollitavus. Muudatuste teostamiseks tuleb koostada tegevusplaan. Muudatuste tegemisest peab säilima kontrolljälg, mis võimaldaks tuvastada muudatuse tegemise aja, teostaja ja muudatuse sisu.

12.2. Infotehnoloogilise süsteemi muudatuste läbiviimisel ja planeerimisel tuleb kindlaks teha, kas ja kuidas muudatused mõjutavad süsteemi turvalisust. Uue riistvara, tarkvara või teenuse hankimist sisaldavate oluliste muudatuste puhul on uute turvanõuete määramiseks vajalik eelnev analüüs. Planeeritud muudatused süsteemi riist- ja tarkvaras peavad olema eelnevalt testitud. Erakorraliste ja planeeritud muudatuste paigaldamine peab olema kooskõlastatud.

IV osa Tarnimine ja tugi

13. Väliste teenusepakkujate kasutamine

13.1. Ettevõttes peavad olema rakendatud väliste teenusepakkujate valikuprotseduurid, mis tagaksid ettevõttele toimiva ja tõhusa teenuse kasutamise.

13.2. Ettevõtte protseduurid peavad tagama, et kõikide väliste teenusepakkujatega oleksid sõlmitud lepingud ning et regulaarselt toimuks osutatavate teenuste vastavuse ülevaatamine lepingu tingimustega ja ettevõtte vajadustega.

13.3. Kõik välised teenusepakkujad peavad olema identifitseeritud ning organisatsioonilised seosed ja tehnilised liidesed nendega peavad olema dokumenteeritud.

13.4. Välistele teenusepakkujatele ei tohi lubada juurdepääsu organisatsiooni vahenditele enne vajalike turvameetmete teostamist ja pääsutingimusi määratleva lepingu allakirjutamist.

14. Mahtude ja jõudluse haldus

14.1. Ettevõttes peab toimima protsess infosüsteemi jõudluse monitoorimiseks ning raporteerimiseks. Regulaarselt tuleb vaadata üle ja määrata kindlaks kasutajate nõudmised infosüsteemi kättesaadavusele ja jõudlusele. Olemasoleva süsteemi jõudluse monitoorimise ja tulevaste jõudlusvajaduste prognoosimise tulemuste põhjal peab olema tagatud infosüsteemi jõudlusvajaduste õigeaegne rahuldamine.

15. Talitluspidevus

15.1. Ettevõttes peab olema toimiv talitluspidevuse planeerimise protsess, mis võtab arvesse äriprotsesside kriitilisust ning tagab pidevusplaanide välja töötamise.

15.2. Talitluspidevuse planeerimine peab hõlmama meetmeid riskide tuvastamiseks ja vähendamiseks, kitsendama õnnetuse võimalikke tagajärgi ning tagama oluliste operatsioonide kiire jätkamise.

15.3. Talitluspidevusplaane tuleb nende tõhususe ja asjakohasuse tagamiseks regulaarselt testida ning vajaduse korral täiendada.

15.4. Ettevõttes peavad olema dokumenteeritud ja juurutatud varukoopiate tegemise protseduurid ning tagatud regulaarne varukoopiate tegemine. Varukoopiaid tuleb teha regulaarselt ning hoida neid eraldiasetsevas hoiuruumis, 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 perioodiliselt kontrollida.

16. Süsteemide turvalisus

16.1. Ettevõtte üldised infoturbe põhimõtted tuleb fikseerida infoturbepoliitikas. Juhtkond peab seadma poliitikaga kindla sihi, näitama toetust ja abi infoturbe tagamisele organisatsioonis. Infoturbepoliitikas peab olema defineeritud infoturbe mõiste, näidatud ära, milliste meetmetega tagatakse infoturve, kes on infoturbe tagamise eest vastutav ning samuti viide ettevõttes kehtestatud tegevuskavadele ja protseduuridele, mis toetavad infoturbe rakendamist. On soovitav, et vastutus infoturbe koordineerimise eest oleks määratud ühele juhtkonna liikmele.

16.2. Organisatsiooni infoturbepoliitikas määratletud konfidentsiaalsusnõuded, turvarollid ja vastutus peavad olema iga töötaja jaoks fikseeritud.

16.3. Ettevõttes peavad pääsuõiguste jaotuse reguleerimiseks olema rakendatud ametlikud protseduurid, mis hõlmavad pääsu elutsükli kõiki faase alates uute kasutajate esialgsest registreerimisest kuni nende kasutajate lõpliku väljaregistreerimiseni, kes infoteenuseid enam ei vaja. 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. Dokumenteeritud ja reaalselt antud pääsuõiguste vastavust tuleb regulaarselt kontrollida.

16.4. Enne kasutajatele infoteenustele juurdepääsu andmist peavad nad saama asjakohase väljaõppe nii organisatsiooni poliitika ja protseduuride alal (kaasa arvatud turvanõuded ja muud talitlusmehhanismid) kui ka infotehnoloogiavahendite õige 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.

16.5. Ettevõttes tuleb tagada tundlike andmete kaitse nende edastamisel avaliku võrgu kaudu. Tundlike andmete edastamisel üle avaliku võrgu tuleb välistada andmete avalikuks tulemise võimalus kolmandatele isikutele.

16.6. Volitamata toimingute õigeaegseks avastamiseks ning rakendatud juurdepääsukontrolli meetmete tõhususe hindamiseks peab olema rakendatud sobiv süsteemipääsu ja –kasutuse seire. Seire korraldamiseks on vajalik infosüsteemis läbiviidavate toimingute kontrolljälg. Infosüsteemi osade vajalik seiretase tuleb määrata riskihinnangute alusel. Turbe rikkumisel on vaja tagada sellest viivitamatu teavitamine ja meetmete rakendamine.

16.7. Ründetarkvara ja viiruste õigeaegseks avastamiseks ja tõkestamiseks peavad olema rakendatud vajalikud meetmed ning määratud vastutus.

17. Konfiguratsioonihaldus

17.1. Ettevõttel peab olema kasutatava infotehnoloogilise riistvara ja tarkvara konfiguratsiooni täielik ja regulaarselt täiendatav inventariloend. Kasutatav riist- ja tarkvaraline platvorm tuleb võimalusel standardiseerida.

17.2. Ettevõttes peavad olema kehtestatud nõuded, mis välistaksid volitamata ja litsentseerimata tarkvara kasutuselevõtu. Ettevõtte peab teostama rutiinseid kontrolle volitamata tarkvara avastamiseks ja litsentsilepingute vastavuse kontrolliks.

18. Probleemide ja intsidentide haldus

18.1. Turvarünnetest, avariidest ja tõrgetest tingitud kahjude vähendamiseks, turvaintsidentide registreerimiseks, neile reageerimiseks ning nendest järelduste tegemiseks peavad olema kehtestatud ametlikud protseduurid ning töökohustused.

18.2. Kõigile asjaomastele töötajatele ja lepingupartneritele tuleb teatavaks teha teavitamisprotseduur eri tüüpi turvaintsidentide (turberikkumine, oht, defekt või tõrge) osas, mis võivad mõjutada organisatsiooni varade turvalisust. Igast avastatud või kahtlustatavast turvaintsidentidest tuleb teatada vastavasse teabepunkti nii kiiresti kui võimalik.

19. Ruumide haldus

19.1. 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.

20. Ekspluatatsiooni haldus

20.1. Põhilisi tüüpseid IT-operatsioone tuleb regulaarselt dokumenteerida ja läbi vaadata, et tagada töötluse plaanipärasus (ajastuse, järjestuse, kvaliteedi jne mõttes). Töötluse õigsuse ja täielikkuse kindlustamiseks tuleb kontrollida ekspluatatsioonilogisid.

V osa Seire

21. Seire ja hindamine

21.1. Ettevõttes peavad olema kehtestatud nõuded infotehnoloogiaalase tegevuse kontrolliks ja hindamiseks. Hinnata tuleb, kas infotehnoloogiaalases tegevuses on järgitud ettevõtte siseselt kehtestatud nõudeid, IT teenuste tõhusust ja IT tegevuse vastavust ärieesmärkidele. Hinnangu andmisel peab olema tagatud selle sõltumatus.

21.2. Infotehnoloogia juhtimismehhanismide, infotehnoloogiat puudutavate õigusaktide ja eeskirjade vastavuse ning infotehnoloogiaalaste lepinguliste kohustuste täitmise hindamiseks tuleb vajadusel kasutada välist auditit. Hindamise tulemused tuleb esitada ettevõtte juhtkonnale.

VI osa Lõppsätted

22. Juhendi jõustumine

22.1. Juhend jõustub alates 01.01.2005.