Finantsinspektsioon

Finantsinspektsiooni soovituslik juhend

Tallinn

NÕUDED FINANTSJÄRELEVALVE SUBJEKTI INFOTEHNOLOOGIA JA INFOTURBE KORRALDUSELE

Soovituslik juhend on kehtestatud Finantsinspektsiooni juhatuse 23. jaanuari 2017 otsusega nr 1.1-7/19 ja muudetud Finantsinspektsiooni juhatuse 12.02.2018 otsusega nr. 1.1-7/43, juhatuse 23.03.2020 otsusega nr. 1.1-7/41 ja 08.06.2020 juhatuse otsusega nr. 1.1-7/77 Finantsinspektsiooni seaduse § 57 lõike 1 ja lõike 3 alusel.

SISUKORD

1. Üldsätted ja mõisted

1.1. Pädevus

1.1.1. Finantsinspektsiooni seaduse (edaspidi *FIS*) § 3 lõike 1 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.

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

1.2. Eesmärk ja kohaldamisala

1.2.1. Käesoleva juhendi (edaspidi *Juhend*) eesmärgiks on sisustada infotehnoloogia ja infoturbe korralduse miinimumnõuded finantssektori ettevõtete tehnoloogiaalaseks töökorralduseks, et seeläbi suurendada finantssektori efektiivsust ja vähendada süsteemseid ning operatsioonilisi riske.

1.2.2. Juhend reguleerib FIS § 2 lõike 1 alusel finantsjärelevalve subjektina käsitletavate isikute v.a krediidiasutuse, makseteenuse pakkuja, investeerimisühingu, krediidiagendi, kindlustusagendi, tegevusloata väikefondi valitseja, investeerimisagendi ja makseagendi infotehnoloogia ja infoturbe korraldust.

1.2.3. Juhendis on kirjeldatud Finantsinspektsiooni hinnangu kohaseid minimaalsed nõuded järelevalvesubjekti infotehnoloogia ja infoturbe korraldusele. Juhendis kehtestatud soovituste ja nõuete kujundamisel on kasutatud rahvusvaheliselt tunnustatud standardites ISO/IEC 27001 ja ISO/IEC 27002 toodud soovitusi.

1.2.4. Juhendi nõuete sisustamisel ja vastavate lahenduste väljatöötamisel ning rakendamisel konkreetse järelevalvesubjekti poolt tuleb arvestada nii subjekti äritegevuse iseloomu, ettevõtte mõju kogu finantssektorile tervikuna kui ka riskide ja nende realiseerumise tagajärgede kaalukust.

1.2.5. Juhendi rakendamisel tuleb arvestada õigusaktidest tulenevate nõuete ja teistest Finantsinspektsiooni juhenditest tulenevate suunistega. Õigusaktidest tulenevate erinõuete korral tuleb lähtuda õigusaktides sätestatust.

1.2.6. 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.

1.2.7. Finantssektori ettevõtte infotehnoloogia ja infoturbe korraldus peab tagama sobiva toe äriprotsessidele. Ettevõtte infosüsteemid peavad vastama äritegevusest ja välistest nõuetest tulenevatele käideldavuse, tervikluse ja konfidentsiaalsuse nõuetele. Juhendi rakendamine ettevõttes sõltub eelkõige ettevõtte protsesside keerukusest ja tagajärgede kaalukusest.

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

1.3. Mõisted

1.3.1. **Auditijälg** on olulise sündmuse toimumist tõendav andmeelement; nähtav jälg või asitõend, mis võimaldab lausungites või aruannetes oleva teabe päritolu jälitada ta algallikani.

1.3.2. **Ettevõte** on Juhendi tähenduses FIS § 2 lõike 1 alusel finantsjärelevalve subjektina käsitletavad isikud v.a krediidiasutus, makseteenuse pakkuja, investeerimisühing, krediidiagent, kindlustusagent, tegevusloata väikefondi valitseja, investeerimisagent ja makseagent.

1.3.3. **Infovara** on informatsioon, andmed ja nende töötlemiseks vajalikud infotöötlusvahendid, mis võivad kuuluda ettevõttele või olla ettevõttes vastutaval hoiul (näiteks isikuandmed).

1.3.4. **Infovara omanik** on ettevõtte töötaja, kes kinnitab infovaraga seotud turvameetmed, volitab juurdepääsu infovarale ja seirab infoturbe meetmete toimivust.

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

1.3.6. **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.

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

1.3.8. **Intsident** on soovimatu sündmus, mille tagajärjeks on (või võib olla) infoturvalisuse rikkumine või ettevõtte tegevuse kahjustamine.

1.3.9. **Krüpteerimine** on andmete teisendamine nende teabesisu peitmiseks, nende volitamata kasutamise vältimiseks või nende märkamatu muutmise vältimiseks.

1.3.10. **Logi** on kronoloogiline sündmuste andmik, mis talletatakse andmefailina järgnevaks läbivaatuseks ja analüüsimiseks.

1.3.11. **Multiautentimine** on autentimine vähemalt kahe sõltumatu autentimisteguriga.

1.3.12. **Oluline intsident** on selline intsident, mille korral kehtib vähemalt üks järgmistest tingimustest:
- > 25 % tavapärasest teenusest on mõjutatud või on suure tõenäosusega mõjutatud;
- > 25 % klientidest on mõjutatud või on suure tõenäosusega mõjutatud;
- intsidendil on oluline majanduslik mõju;
- intsident on eskaleeritud kõrgeimale juhtimistasandile ning ettevõte on rakendanud talitluspidevusplaani;
- intsidendiga kaasneb või võib kaasneda oluline mainekahju;

või samaaegselt vähemalt kolm järgnevalt loetletud tingimust:
- > 10 % tavapärasest teenusest on mõjutatud või on suure tõenäosusega mõjutatud;
- > 10 % klientidest on mõjutatud või on suure tõenäosusega mõjutatud;

- intsident on põhjustanud > 2 tunni kestva teenuse katkestuse;
- intsident on eskaleeritud kõrgeimale juhtimistasandile;
- intsidendil on mõju teistele teenuseosutajatele või asjakohasele taristule;
- intsidendiga kaasneb või võib kaasneda mainekahju.

1.3.13. **Tundlik informatsioon** on informatsioon, mille konfidentsiaalsust ja terviklust vastavalt ettevõtte pädeva organi otsusele tuleb kaitsta, sest selle avalikustamine, muutmine, hävimine või kadumine põhjustaksid olulist kahju.

1.3.14. **Turvaala** on ala, kuhu paigutatakse kriitilised infrastruktuuri komponendid ja mille kaitseks rakendatakse eraldi turvameetmed.

1.3.15. **Võtmehaldusprotsess** on krüptovõtmete ja nende turvameetmetega seotud tegevused võtme kogu elutsükli jooksul.

2. Dokumentatsioon ja korraldus

2.1. IT strateegia

2.1.1. Ettevõtte infotehnoloogiaalase tegevuse aluseks peab olema juhtkonna poolt kinnitatud ärieesmärkidest ja -strateegiast lähtuv strateegia (IT strateegia). IT strateegia loomisel tuleb hinnata, millist tehnoloogilist tuge on vaja ettevõtte ärieesmärkide saavutamiseks, ning kas olemasolevad IT lahendused võimaldavad saavutada soovitud ärilist tulemust. Ettevõtte strateegiline plaan peab olema piisavalt detailne võimaldamaks määratleda konkreetseid arenguplaane ning määratleda IT projektide prioriteedid ja investeeringud.

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

2.2. Infoturbe poliitika

2.2.1. Ettevõtte üldised infoturbe põhimõtted tuleb fikseerida infoturbe poliitikas, mille kinnitab kõrgem juhtkond. Infoturbe poliitika eesmärk on määratleda ettevõtte strateegiline lähenemisviis infoturbe korraldamisele.

2.2.2. Infoturbe poliitika peaks sisaldama vähemalt järgmiseid sätteid:

- infoturbe määratlus, eesmärgid ja põhimõtted, mis suunavad infoturvet mõjutavaid tegevusi;
- kindlaksmääratud rollidele üldiste ja konkreetsete kohustuste määramine infoturbe haldamiseks;
- protsessid, millega käsitletakse kõrvalekaldeid ja erandeid.

Madalamal tasemel peaks infoturbe poliitikat toetama teemaspetsiifilised poliitikad, sh infoturbe rakendamist toetavad tegevuskavad, standardid, protseduurid ja juhendid.

2.2.3. Ettevõtte töötajad ja asjassepuutuvad välised osapooled peavad olema teadlikud ning aru saanud organisatsioonis kehtivast infoturbe poliitikast ja sellest tulenevatest alamdokumentidest ning töötajate rollist ja vastutusest infoturbe tagamisel. Infoturbe poliitika olulise muudatuse korral tuleb sellest teavitada töötajaid ja asjassepuutuvaid väliseid osapooli. Uue töötaja värbamisel tuleb talle tutvustada kehtivat infoturbe poliitikat, alamdokumente ning tema rolli ja vastutust infoturbe tagamisel.

2.2.4. Lähtuvalt ettevõtte tegevusvaldkonnast, äri- ja IT strateegiast ning riskitaluvusest tuleb kehtestada sobivad infoturbe poliitika ülevaatamise põhimõtted, sh nende sagedus. Ettevõttes

peab toimima regulaarne infoturbe poliitika ülevaatamine ning iga suurema muudatuse korral ettevõtte äritegevuses või infotehnoloogia korralduses vajaduse korral infoturbe poliitika täiendamine.

2.3. Sise-eeskirjad ja protseduurid

2.3.1. Ettevõttes tuleb kehtestada ajakohased, sobivad ja adekvaatsed sise-eeskirjad, millega tagatakse, mh infosüsteemi arendamisel, haldusel ja kasutamisel, andmete konfidentsiaalsus, käideldavus ja terviklus ning kindlustatakse andmete töötluse vastavus kehtivatele õigusnormidele ja parimatele tavadele.

2.3.2. Ettevõttel tuleb tagada sise-eeskirjade aja- ning asjakohasus. Infosüsteemis muudatuste tegemisel tuleb üle vaadata ka vastavad protseduurid ning teavitada kasutajaid teostatud muudatustest.

2.4. Investeeringute juhtimine

2.4.1. Tehnoloogiasse ja infoturbesse tehtavate kulutuste ärieesmärkidele vastavaks ja optimaalseks juhtimiseks peab investeeringute juhtimine toimuma läbi perioodiliselt toimuva eelarvestamise protsessi.

2.4.2. Juhtkond peab vähemalt üks kord aastas analüüsima ettevõtte infotehnoloogia ja infoturbe korraldust. Soovitav on regulaarselt üle vaadata IT ressursside otstarbekas kasutamine äristrateegiate toetuseks ning kinnitada järgmise perioodi eelarve.

3. Personal

3.1. IT organisatsioon

3.1.1. Protsessidele vajaliku infotehnoloogilise toe osutamiseks peab ettevõttes olema suuruselt ja kompetentsilt sobiv IT organisatsioon. Kui infotehnoloogia-alane oskusteave ostetakse väljastpoolt, tuleb määrata valdkonnad, kus võib kasutada teenuse sisse ostmist ning kelle poolt ja kuidas teenust hallatakse.

3.1.2. IT personali värbamiseks peab ettevõttes kehtestama asjakohased protseduurid, mis võimaldavad hinnata isiku sobivust vastavale ametikohale. Arvesse tuleb võtta lisaks erialasele kompetentsusele ka vajadust töötada tundliku informatsiooniga ja ettevõtte tegutsemissfääri.

3.1.3. Ettevõtte IT organisatsioonil peab olema selgelt määratletud struktuur ja ülesanded ning oma kohustuste täitmiseksvajalik ressurss.. Töötajate nõutavad oskused, õigused, vastutus ja kohustused tuleb selgelt määratleda ning regulaarselt üle vaadata.

3.1.4. Ettevõttes peab rakendama infotehnoloogia arenduse ning halduse funktsioonide lahusust. Juhul kui töökohustuste lahususe sisse viimine ei ole võimalik, tuleb rakendada riskide maandamiseks teisi täiendavaid kontrolle arvestades asjaolu, et töötaja ei tohi teostada kontrolli ega järelevalvet oma tegevuse üle.

3.1.5. Ettevõttel tuleb määratleda ja välja selgitada kesksed IT-töötajad ning rakendada täiendavaid kontrolle minimeerimaks ülemäärast sõltuvus neist.

3.2. Infoturbe organisatsioon

3.2.1. Üldine vastutus infoturbe tagamise eest on ettevõtte juhatusel. Ettevõttes tuleb eraldi määrata infoturbe eest vastutav isik – infoturbejuht. Lähtuvalt organisatsiooni suurusest ja tegevuse keerukusest võib osutuda asjakohaseks eraldi ametikoha loomine. Infoturbejuht peab alluma

vahetult sellisele tasandile ettevõttes, mis võimaldab infoturbejuhile pandud ülesandeid täita. On soovitav, et vastutus infoturbe koordineerimise eest oleks määratud ühele juhtkonna liikmele.

3.2.2. Ettevõtte ärivaldkonna kaasamiseks infoturbega seotud küsimustesse on soovitatav moodustada infoturbe juhtrühm (*steering commitee*), kuhu peaksid kuuluma kõigi oluliste äriüksuste või funktsioonide juhid ning infoturbejuht.

3.2.3. Infoturbejuhi ja IT riskijuhtimise funktsioonide rakendamise kaudu peab ettevõte tagama vähemalt järgneva:

- infovarade identifitseerimise ning klassifitseerimise, infoturbeprotsesside (sh IT riskijuhtimine) toimimise;
- infovara omanike määramise;
- infoturbega seotud ajakohase dokumentatsiooni olemasolu ning selle rakendamise;
- infoturbe korralduse vastavuse tagamise infoturbe poliitikale, sisemistele kordadele ning välistele nõuetele asjakohaste organisatoorsete, füüsiliste ja infotehnoloogiliste infoturbemeetmete rakendamise kaudu;
- juhtkonna teavitamise regulaarselt, kuid mitte harvem kui kord aastas, ettevõtte turvataseme vastavusest ettevõtte sisestele ja välistele nõuetele ning rakendatud infoturbemeetmete tõhususest;
- juhtkonna teavitamise olulistest infoturbeintsidentidest ning nende lahendamisest;
- infosüsteemide arendamisel või muutmisel turvaaspektidega arvestamise;
- infosüsteemide talitluspidevuse ja taasteprotsesside toimimise;
- töötajate teavitamise turvareeglitest, nende nõustamise infoturbealastel teemadel ning vajaduse korral ettevõtte töötajatele koolituse korraldamise üldise turvateadlikkuse tõstmiseks.

3.3. Töötajad

3.3.1. Ettevõttes tuleb kehtestada mehhanismid vastutavatele ametikohtadele võetavate töötajate (nt ettevõtte infosüsteemides eriõigusi omavad töötajad) tausta kontrollimiseks. Arvesse tuleb võtta lisaks erialasele kompetentsusele ka vajadust töötada tundliku informatsiooniga ja ettevõtte tegevusvaldkonda.

3.3.2. Enne kasutajatele infovarale juurdepääsu andmist peab tagama nende informeerituse 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 juhtkonda) ning mis tutvustaksid eeskätt ettevõtte infoturbepoliitikat, infoturbe tähtsuse põhjuseid, sellega seotud kohustusi ning protseduure, turvanõudeid, intsidentidest teavitamist jms.

3.3.3. Ettevõtte töötajatega sõlmitavates töölepingutes tuleb sätestada muuhulgas konfidentsiaalse informatsiooni hoidmise kohustus ja selle kohustuse rikkumisega kaasnev vastutus ka pärast töötaja lahkumist ettevõttest.

3.3.4. Töötaja õigused, kohustused ja vastutuse peab määratlema infoturbe juhendites ja muudes asjakohastes siseregulatsioonides.

3.3.5. Iga töötaja jaoks tuleb fikseerida organisatsiooni infoturbe poliitikas määratletud konfidentsiaalsusnõuded, turvarollid ja vastutus. Infoturbe tagamine oma tööülesannete täitmisel on iga töötaja kohustus ja see peab selgelt väljenduma nii organisatsiooni kultuuris kui ka töötajatega sõlmitavates lepingutes ja kokkulepetes.

3.4. Välise teenusepakkuja kasutamine

3.4.1. Ettevõte vastutab väliselt teenusepakkujalt ostetud teenuse toimimise eest samas ulatuses nagu ise seda osutades. Tegevusjuhised ja -suunised järelevalvesubjekti tegevuse edasiandmiseks on kehtestatud Finantsinspektsiooni juhendiga „Nõuded finantsjärelevalve subjekti poolt tegevuse edasiandmisele (*outsourcing*)".

3.4.2. Enne teenuse või toote ostmise või jätkuvat tegevuse edasiandmise (edaspidi käesolevas punktis teenuse ostmine ja tegevuse edasiandmine ühiselt *teenuse ostmine*) otsustamist peab ettevõte määratlema nõuded teenuse või toote sisule, kvaliteedile ja turvalisusele, hindama kaasnevaid riske ja võimalikke teenusepakkujaid. Teenuse ostmise puhul tuleb täpsustada teenuse lõpetamise strateegiat juhuks, kui leping lõpetatakse.

3.4.3. Ettevõte peab regulaarselt hindama välise teenusepakkuja kasutamisest tulenevaid riske, muuhulgas riske turvalisusele. Sellist hindamist tuleb teha nii välise teenusepakkuja valikul, lepingu sõlmimisel kui ka vastava teenustaseme leppe (SLA) kokkuleppimisel. Vastavalt teenuse olemusele tuleb kindlaks määrata, millistele turvalisuse nõuetele peab teenusepakkuja vastama. Kui infosüsteemi arendatakse või hallatakse välise teenusepakkuja poolt, ei tohi süsteemi minimaalne infoturbe tase olla madalam ettevõtte määratud teenusetaseme nõuetest. Ettevõtte peab kehtestama kontrollimehhanismi, mis tagab välise teenusepakkuja infoturbe võimekuse hindamise.

3.4.4. Ettevõtte ja välise teenusepakkuja vahelises lepingus peab täpselt määratlema teenuse sisu ja selle ulatuse. Lepingus peab detailselt määratlema teenuse kirjelduse, turvanõuded, konfidentsiaalsuskohustused, ettevõtte õiguse saada teenuse monitoorimiseks vajalikku informatsiooni, teenusepakkuja kohustus viivitamatult teavitada intsidentidest ning lepingu muutmise, lõppemise ja lõpetamise (sh nii korralise kui ka erakorralise) alused, tingimused ja kord.

3.4.5. Välise teenusepakkujaga suhtlemise protsess peab olema formaliseeritud. Teenuse seireks peab ettevõttes toimima protsess, et hinnata välise teenusepakkuja poolt ärinõuete, lepingu sätete ning teenustaseme lepete täitmist.

3.4.6. Teenuse ostmisel, sh pilvtöötluse puhul, on ettevõte kohustatud säilitama piisava kontrolli ettevõtte klientide andmeid hõlmava informatsiooni üle, sh nende andmete edastamist, asukohta ja säilitamist. Ettevõtte infosüsteemid peavad olema vähemalt loogiliselt turvalisel viisil eraldatud välise teenusepakkuja teiste klientide infosüsteemidest.

3.4.7. Ettevõte peab tagama, et väliste teenusepakkuja kasutamisel on lepinguga kehtestatud ettevõttele ja järelevalvele vajalikud ja piisavad õigused kontrollimaks ja hindamaks teenusepakkuja tegevust ning teenusepakkuja kohustus alluda sellisele kontrollile ja teha koostööd. Nimetatud õigused peavad hõlmama muuhulgas õigust saada ammendavat teavet teenusepakkuja tegevuse kohta (teenusepakkuja aruandluskohustus), anda täiendavaid juhiseid teenuse osutamiseks ja nõuda selliste juhiste täitmist. Ettevõte peab teostama järelevalvet ostetud teenuse kvaliteedi ja turvalisuse üle.

4. Infovarad ja riskihaldus

4.1.1. Ettevõtte juhatus peab tagama infotehnoloogia-alaste riskide haldamise protsessi, mis määratleb riskide juhtimise metoodika, aruandekohustuse ja kontrollmehhanismid, toimimise. Kasutatav riskianalüüside metoodika peab olema dokumenteeritud.

4.1.2. Ettevõtte juhatus peab tagama üldised reeglid ja vastava protsessi toimimise infovarade klassifitseerimiseks ja neile omanike määramiseks.

4.1.3. Infovara omaniku kohustused võiksid olla vähemalt järgnevad:

- enda infovaraga seotud riskianalüüsides osalemine ja selle tulemite aktsepteerimine;
- riskianalüüside alusel rakendatavate turvanõuete ja jääkriski aktsepteerimine;
- IT teenuste osas teenustaseme lepete (SLA) sõlmimine ja kinnitamine;
- enda infovaraga seotud muudatuste tellimine, prioritiseerimine ja kooskõlastamine;
- enda infovaradega seotud juurdepääsuõiguste reguleerimine ja volitatud töötajate tegevuse kontrollimine;
- auditijälje osas nõudmiste kehtestamine.

4.1.4. Riskianalüüsi käigus tuleb ettevõttel välja selgitada infovarasid mõjutavad 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.

4.1.5. Infosüsteemide turvalisuse vajadus ja vastavad kontrollid ja meetmed peab määrama koostöös infovara omanikuga.

4.1.6. Riskide hindamisel tuleb muu hulgas arvesse võtta ettevõtte tehnilistest lahendustest, protsessidest, välistest osapooltest tulenevaid riske kui ka infosüsteemide monitooringu tulemusi.

4.1.7. Lähtuvalt riskianalüüsi tulemustest peab ettevõte kehtestama, juurutama ja rakendama turvameetmeid infovaradele.

4.1.8. Iga olulise muudatusega infosüsteemis või protsessis peab kaasnema riskide hindamine. Infotehnoloogilise süsteemi muutuste planeerimisel tuleb kindlaks teha, kas ja kuidas mõjutab muudatus süsteemi ja protsessi turvalisust, ning vähendada igakülgselt muudatusega kaasnevate riskide mõju.

4.1.9. Ettevõte peab tagama riskihinnangute regulaarse uuendamise (vähemalt kord aastas) ning riskide haldamise protsessi järjepidevuse. Riskide hindamine peab toimuma kogu infosüsteemi elutsükli vältel, st infosüsteemi arendamisel, muudatuste teostamisel, oluliste ohtude ilmnemisel, oluliste intsidentide realiseerumisel või nende hulga arvulisel suurenemisel. Riskihinnangute tulemuste alusel tuleb vajadusel täiendada infovarade turvalisuse ja kontrollialaseid meetmeid.

4.1.10. Riskianalüüside tulemused ning asjakohased ülevaated tuleb esitada ettevõtte juhtkonnale.

5. Füüsiline ja keskkonna turve

5.1. Turvapiirkonnad

5.1.1. Ettevõttel tuleb kaardistada piirkonnad, mida infoturbe seisukohast tuleb kaitsta ja kuhu tohivad siseneda vaid selleks volitatud isikud. 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.

5.1.1. Piiratud juurdepääsuga turvaalade kaitseks tuleb kasutada sobivaid füüsilisi ja loogilisi juurdepääsukontrolle selliselt, et ainult volitatud isikud saaksid piirkonda sissepääsu.

5.1.2. Piiratud juurdepääsuga turvaalasid tuleb pidevalt monitoorida võimalike kahjustuste ennetamiseks, kahjustuste tekkimisel kiireks avastamiseks ja reageerimiseks.

5.1.3. Turvaalade kaitsmiseks on turvameetmete valimisel soovitav võtta aluseks mõne sõltumatu ja tunnustatud organisatsiooni poolt kirjeldatud standardid. Turvameetmeid tuleb arvesse võtta juba turvalise piirkonna asukoha valikul ja rakendada selle väljaehitamisel ning sisustamisel.

Serverimajutusteenuse edasiandmisel peavad teenusepakkuja ja pakutava lahenduse valikul kehtima samad standardid.

5.1.4. Turvaliste piirkondade puhul tuleb vältida nende tähistamist üldarusaadavalt ja kandmist viitadele.

5.1.5. 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.

5.2. Arvutivõrgu turvalisus

5.2.1. Ettevõte peab omama ajakohast ülevaadet oma arvutivõrgust ja juurdepääsuskeemidest.

5.2.2. Võrguturbe meetmed tuleb kehtestada nii võrku pääsemise, võrgus kasutatavate teenuste kui ka võrgus teostavate toimingute kohta.

5.2.3. Ettevõtte arvutivõrk peab olema piisavalt füüsiliselt ja loogiliselt segmenteeritud, et oleks tagatud kehtestatud käideldavuse, konfidentsiaalsuse ja tervikluse nõuete täitmine. Lokaalse arvutivõrgu ja välise arvutivõrgu vahelisse andmevoogu tohib lubada ainult teenuseid, mis on vajalikud ettevõtte funktsioonide täitmiseks.

5.2.4. Andmete kaitseks peavad ettevõtte arvutivõrgus olema kasutusel piisavalt turvalised võrguprotokollid ning adekvaatsed ja tugevad krüpteerimisalgoritmid.

5.2.5. Ettevõttes tuleb tagada andmete turvalisus nende edastamisel avaliku või raadiovõrgu 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.

5.2.6. Ettevõte peab tagama piisava võrgu seire ning logimise, et tuvastada ja jäädvustada võimalikud infoturvet mõjutavad toimingud ning nõrkused. Võrguliikluse jälgimiseks ja väärkasutuse kahtluse korral vastutavate isikute teavitamiseks tuleks kasutusele võtta ning ajakohasena hoida rünnete tuvastamise süsteemid (IDS – *intrusion detection system*) ja rünnete tõrje süsteemid (IPS – *intrusion prevention system*).

5.2.7. Ründetarkvara ja viiruste õigeaegseks avastamiseks ja tõkestamiseks peab rakendama vajalikke meetmeid ning määrama vajalikud töötaja vastutused. Lisaks tuleb viivitamatult teavitada kasutajaid ründetarkvara ja viirustega kaasnevast ohust, kui adekvaatsest infoallikast pärineva teabe põhjal on ründetarkvara ja viiruste levikust tulenev reaalne oht ettevõttele suurenenud.

5.2.8. Juhul kui infosüsteemide administreerimist teostatakse kaugjuurdepääsu kaudu, peab tegevus olema kaitstud asjakohaste krüptograafiliste (nt VPN) ja turvalise autentimise lahendusega.

5.2.9. Traadita andmeside tehnoloogia kasutamisel tuleb rakendada vajalikke meetmeid vältimaks autoriseerimata juurdepääsu infosüsteemidele.

5.2.10. Ettevõte võiks regulaarselt kontrollida arvutivõrku võimalike sise- või väliskeskkonnast tulenevate nõrkuste suhtes või pärast suuremaid muudatusi võrgus (uue süsteemi või seadme lisamisel, võrgu topoloogia muutudes, tulemüüri seadete muutudes, pärast uuenduste installeerimist) ning võimalusel viia läbi võrgu infrastruktuuri ründeteste (*penetration test*).

5.3. Seadmete turvalisus

5.3.1. Ettevõte peab määratlema, kas ettevõtte infovarade kasutamine mobiilse seadme kaudu on lubatud arvestades ettevõtte vajadusi, seadmete kasutusest tulenevaid riske ning IT osakonna suutlikkust.

5.3.2. Ettevõte peab määratlema, millist informatsiooni võib salvestada lokaalsetesse ja mobiilsetesse seadmetesse ning kuidas seda tuleb kaitsta.

5.3.3. Kui ettevõtte infosüsteemile on lubatud kaugligipääs, peavad ettevõttel olema asjakohased turvameetmed vältimaks kolmanda isiku ligipääsu tundlikule infole.

5.3.4. Ettevõttele kuuluvasse seadmesse tohib installeerida ja kasutada ainult ettevõtte poolt aktsepteeritud tarkvara ning konfiguratsiooni. Ettevõte peab kehtestama protseduurid ning rakendama asjakohaseid meetmeid kaitsmaks seadmeid turvaohtude eest.

5.3.5. Ettevõttes kasutatavate seadmete funktsionaalsust tuleb piirata tasemeni, mis on vajalik tööülesannete sooritamiseks.

5.3.6. Ettevõte peab tagama, et kui kasutaja jätab seadme aktiivse kasutuseta määratud perioodiks, siis infosüsteemi kasutamise jätkamine või ühendus arvutivõrku on võimalik üksnes pärast kasutajauut autentimist.

5.3.7. Juhul kui töötajatel on lubatud kasutada isiklikke seadmeid töö tegemiseks, peab ettevõttes olema kehtestatud isikliku seadme kasutamise eeskiri, kus on täpselt määratletud andmete hoidmise, edastamise, seadme hoolduse ja turvalisuse nõuded. Nimetatud eeskiri ja isiklikus seadmes rakendatavad meetmed ei tohi vähendada ettevõttes kehtestatud infoturbe taset.

5.3.8. Töötajad peavad saama piisavat juhendamist ja turvaalaseid koolitusi eelnimetatud eeskirja, selle rakendamise ja isikliku seadmete lubatud kasutamise kohta.

5.4. Andmekandjate turvalisus

5.4.1. Ettevõte peab kehtestama eeskirja, mis reguleerib andmekandja kasutamist ja levitamist organisatsioonis ning kolmandatele isikutele. Eeskirjaga tuleb kehtestada ja rakendada nõuded andmekandja kasutamiseks, säilitamiseks ning turvaliseks hävitamiseks.

5.4.2. Ettevõte peab kehtestama ja rakendama sobivaid meetmeid andmekandjate kaitseks.

5.4.3. Andmekandjal oleva info kaitsmiseks tuleb võimalusel rakendada sobivaid infotehnoloogilisi meetmeid (nt andmete krüpteerimine).

5.4.4. Andmekandja edastamisel tuleb kasutada usaldusväärset ja turvalist kullerteenust, millest on võimalik omada täpset ülevaadet.

6. Side ja operatsioonide haldus

6.1. Mahtude ja jõudluse haldus

6.1.1. Ettevõttes peab toimima protsess infosüsteemi jõudluse monitoorimiseks ning raporteerimiseks. Regulaarselt tuleb üle vaadata ja määrata kindlaks kasutajate nõudmised infosüsteemi kättesaadavusele ja jõudlusele. Olemasoleva süsteemi jõudluse monitoorimise ja tulevaste jõudlusvajaduste prognoosimise tulemuste põhjal peab tagama infosüsteemi jõudlusvajaduste õigeaegse rahuldamise.

6.2. Konfiguratsioonihaldus

6.2.1. Ettevõttel peab olema kasutatava infotehnoloogilise riist- ja tarkvara paigaldamise ja konfiguratsiooni täielik ja regulaarselt täiendatav dokumentatsioon. Kasutatav riist- ja tarkvaraline platvorm tuleb võimalusel standardiseerida.

6.2.2. Tarkvara tehnoloogiast tulenevate nõrkuste kaitseks peab ettevõte kehtestama reeglid tarkvarauuenduste väljaandmise jälgimiseks ja nende testimiseks ning rakendamiseks. Tarkvarauuenduste halduse vastutus peab olema määratud igale eraldiseisvale tarkvaralisele süsteemile.

6.2.3. Infosüsteemi konfiguratsiooni muutmisel tuleb järgida muudatuste halduse protseduuri, mille kaudu oleks tagatud muudatuse mõju eelnev analüüs, dokumenteerimine, testimine ja paigaldamise kooskõlastamine.

6.2.4. Enne süsteemi või seadme ettevõtte võrku installerimist tuleb muuta tootja algseid turvaseadeid (muuta paroole, sulgeda mittevajalikud kontod, vmt).

6.2.5. Ettevõttes peavad kehtima nõuded, mis välistavad volitamata ja litsentseerimata tarkvara kasutuselevõtu. Ettevõtte peab teostama rutiinseid kontrolle volitamata tarkvara avastamiseks ja litsentsilepingute vastavuse kontrolliks.

6.2.6. Ettevõttes tuleb tagada infosüsteemide standardtarkvara ja süsteemi komponentide vajalike uuenduste ja turvapaikade paigaldamise protsessi toimimine. Uued turvapaigad tuleks paigaldada, kui ettevõttes ollakse veendunud kõrvalmõjude puudumises. Uute turvapaikade avalikustamist tuleb perioodiliselt kontrollida. Ettevõtte peab tagama, et minimiseeritakse teadaolevaid turvalisuse nõrkuseid ja rakendatakse hetke parima praktika kohaseid turvameetmed.

6.2.7. Pärast vajalike muudatuste teostamist peab ettevõte tagama standardtarkvara ja süsteemi komponentide funktsionaalsuse piiramise vähimale vajalikule tasemele. Samuti tuleb sulgeda mittevajalikud teenused ja protokollid (need teenused ja protokollid, mis ei ole otseselt vajalikud seadme põhifunktsiooni täitmiseks).

6.3. Muudatuste haldus

6.3.1. Ettevõtte infosüsteemis muudatuste planeerimisel ja läbiviimisel tuleb kindlaks teha nende mõju ettevõttele ja olemasolevatele tehnilistele lahendustele. Mõju arvestamisel on aluseks erinevad tegurid, mida peaks hindama ja analüüsima, sh:

- mõju IT teenusele ja süsteemile ja infrastruktuurile;
- mõju teistele teenustele ja süsteemidele, mis toimivad samas infrastruktuuris;
- mõju süsteemi turvalisusele (uue riistvara, tarkvara või teenuse hankimist sisaldavate oluliste muudatuste puhul on uute turvanõuete määramiseks vaja teostada eelnev analüüs);
- muudatuse mitterakendamise mõju;
- IT ja muud ressursid, mis on vajalikud muudatuse rakendamiseks.

6.3.2. Muudatuste teostamiseks tuleb koostada tegevusplaan. Erakorraliste ja planeeritud muudatuste teostamine peab olema kooskõlastatud ning heaks kiidetud vastava infovara omaniku poolt.

6.3.3. Muudatuste üksikasjadest peab teavitama kõiki asjassepuutuvaid isikuid.

6.3.4. Infosüsteemi muudatuste tagajärjel tekkida võivate katkestuste, vigade ja õigusaktide nõuete rikkumise esinemise tõenäosuse vähendamiseks tuleb kavandatava muudatuse eesmärki

arvestades tagada muudatuste teostamise õiguspärasus ja kontrollitavus. Muudatuste tegemisest peab säilima kontrolljälg, mis võimaldab tuvastada muudatuse tegemise aja, teostaja ja muudatuse sisu.

6.3.5. Planeeritud muudatused süsteemi riist- ja tarkvaras peavad olema eelnevalt testitud. Enne muudatuse teostamist tuleb defineerida asjakohased ennistamisprotseduurid, mida on võimalik ebaõnnestumiste korral koheselt rakendada endise olukorra taastamiseks. Soovitatav on eelnevalt testida ka ennistamiste protseduure.

6.3.6. Ettevõte peab tagama finantsjärelevalvet teostava asutuse haldusaktiga või toiminguga nõutud informatsiooni käideldavuse ja tervikluse aktile või toimingule eelneval määral. Nimetatud nõude rikkumisel infosüsteemi muudatuste tagajärjel või tõenäolisel tagajärjel esitab ettevõte finantsjärelevalve teostajale motiveeritud seletuse muudatuse kohta ja infovara omaniku suhtes rakendatavad õiguskaitsevahendid või muud teod.

6.4. Infosüsteemide seire ja logid

6.4.1. Ettevõttes peab toimima infosüsteemide seire, mis tagab vähemalt infosüsteemide turbe halduses ennetavate meetmete rakendamise ja intsidentide õigeaegse identifitseerimise.

6.4.2. Infosüsteemide seire kaudu peab olema tagatud järgnev:
- sisemiste ja väliste ohtude õigeaegne identifitseerimine;
- infosüsteemide nõrkuste identifitseerimine;
- riist- ja tarkvara autoriseerimata kasutamise tuvastamine ning selle ennetamine;
- infosüsteemide konfiguratsiooni ja seadmete muudatuste monitooring;
- infosüsteemide, seadmete ja protsesside käideldavuse monitooring.

6.4.3. Ettevõte peab rakendama volitamata toimingute õigeaegseks avastamiseks, rakendatud juurdepääsukontrolli meetmete tõhususe hindamiseks ja infosüsteemide vigade tuvastamiseks sobivat süsteemipääsu ja -kasutuse seiret.

6.4.4. Volitamata toiming on iga toiming, millega rikutakse õigusaktide nõudeid või mille eesmärgiks või sisuks on finantsjärelevalve teostaja haldusakti või toimingu ebakohane täitmine või täitmata jätmine, sh informatsiooni tervikluse või käideldavuse rikkumine võrreldes ettevõtte poolt akti saamisele või toimingu tegemisele eelneva ajaga. Finantsjärelevalve asutuse poolt vastava nõude saamisel põhjendab ettevõte detailselt eelmises lauses kirjeldatud volitamata toimingut.

6.4.5. Seire korraldamiseks on vaja omada infosüsteemis läbiviidavate toimingute logi. Infosüsteemi osade sobiv seiretase tuleb määrata riskihinnangute alusel. Ettevõte peab tagama logide piisava analüüsiprotsessi avastamaks vigu süsteemide toimimises või võimalikke informatsiooni käideldavuse, tervikluse või konfidentsiaalsuse rikkumisi.

6.4.6. Ettevõte peab kasutama logide analüüsiks sobivaid meetmeid ja vahendeid. Kõnealused meetmed ja vahendid peavad olema kättesaadavad ainult volitatud personalile.

6.4.7. Vastavalt õigusaktides ning ettevõtte poolt infovarale määratud turvalisuse nõuetele kehtestatakse toimingute liigid, millede teostamise kohta salvestatakse ja säilitatakse kehtestatud tähtaegadeks logid.

6.4.8. Logisid tuleb pidada ettevõttele tähtsa informatsiooni kohta vähemalt järgmiste võimalike toimingute osas (sõltumata toimingu õnnestumisest või ebaõnnestumisest):
- sisenemine süsteemi;
- informatsiooni vaatamine;

- päringute tegemine;
- süsteemi ja aplikatsiooni poole pöördumine;
- andmebaasi muudatused ja tehingud;
- katsed saada ligi tundlikule informatsioonile;
- süsteemide kasutus ja toimingud spetsiaalsete (privilegeeritud) kasutusõigustega;
- autoriseerimata toimingud infosüsteemis.

6.4.9. Logi peab sisaldama vähemalt toimingu teostajat, liiki ja selle teostamise aega.

6.4.10. Logi salvestamisel, haldamisel ja säilitamisel peab olema tagatud selle vältimatus, käideldavus, terviklus ja konfidentsiaalsus. Logifailide andmekandjaid on soovitav hoida turvalises piirkonnas ja eraldi logitavast infotöötluskeskkonnast.

6.4.11. Ajalise täpsuse tagamiseks peavad kõigi protsessiga seotud süsteemide kellad olema sünkroniseeritud.

6.5. Talitluspidevus ja varundus

6.5.1. Tegevusjuhised ja -suunised järelevalvesubjektile talitluspidevuse valdkonna korraldamiseks on kehtestatud Finantsinspektsiooni juhendiga „Nõuded finantsjärelevalve subjekti talituspidevuse protsessi korraldamisele“.

6.5.2. Ettevõte peab dokumenteerima ja juurutama varukoopiate tegemise ja koopiast taastamise protseduurid, kus on määratletud organisatsiooni nõuded teabe, tarkvara ja süsteemide varundamisele ning varundusandmete säilitamisele ja kaitsele. Varukoopiate teostamise ulatus ja sagedus peaksid peegeldama organisatsiooni tegevusest tulenevaid nõudeid, asjassepuutuva teabe turvanõudeid ning teabe elutähtsust organisatsiooni tegevuse jätkamise seisukohalt.

6.5.3. 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 taastamise testimine.

6.5.4. Varukoopiaid tuleb teha regulaarselt ning neid tuleb hoida turvalises piirkonnas, mis välistab volitamata juurdepääsu. Eelnev peab tagama koopiate asjakohasel tasemel füüsilise- ja keskkonnakaitse, mis vastab põhiasukohas rakendatavatele normidele. Ühte eksemplari varukoopiatest tuleb regulaarselt ning turvaliselt ladustada asukohas, mis oleks piisavalt kaugel kahjustuste vältimiseks põhiasukoha avarii korral.

6.5.5. Varukoopiad peavad olema kaitstud autoriseerimata kasutamise ja andmete riknemise eest, vajadusel tuleb varukoopiad kaitsta krüpteerimisega.

6.5.6. Varukoopiate kasutuskõlblikkust ning täielikkust tuleb regulaarselt kontrollida veendumaks, et vajadusel saab neid hädaolukorras usaldada ning et varunduskorraldus vastab ettevõtte talitluspidevuse plaanide nõuetele. Ärikriitiliste süsteemide ja teenuste puhul peaks varunduskorraldus hõlmama kogu süsteemiteavet ning kõiki rakendusi ja andmeid, mis on vajalikud kogu süsteemi taastamiseks avarii korral.

6.5.7. Ettevõte peab määratlema ja kehtestama infovara säilitamise aja arvestades õigusaktide nõudeid, aegumistähtaegu ja finantsjärelevalve asutuse võimalikku huvi info suhtes.

6.5.8. Olukorras, kus ettevõtte töötaja või juhtorgani liige loob või töötleb ametialast infot ettevõtte valduses või kasutuses mitteolevas süsteemis (nt isiklik seade, isiklik postkast teenusepakkuja juures, vmt) ning selle kohene salvestamiskohustus ei tulene õigusaktidest, peab ettevõte tagama nii loodud kui ka töödeldud ametialase info säilitamise esimesel võimalusel ka ettevõtja valduses või kasutuses olevas tehnilises lahenduses.

7. Krüpteerimine

7.1.1. Vastavalt vajadusele ja informatsiooni tundlikkusele, eeskätt konfidentsiaalsuse ja tervikluse tagamiseks, tuleb informatsiooni kaitseks rakendada krüpteerimist.

7.1.2. Ettevõttes tuleb kehtestada reeglid krüpteerimise kasutamiseks. Reeglid peavad sätestama, millisel juhul on andmete krüpteerimine kohustuslik. Samuti peab kokku leppima kasutatava krüptograafiline algoritmi, minimaalsed krüptovõtme pikkused ja tingimused, kuidas krüptograafilisi võtmeid hallatakse.

7.1.3. Ettevõttes kehtestatud võtmehaldusprotsess võiks määratleda, kuidas toimuvad järgmised tegevused:

- krüptovõtmete genereerimine;
- krüptovõtmete jaotamine, säilitamine, muutmine ja hävitamine;
- krüptovõtmete asendamine nende avalikustumise või vastava kahtluse tekkimise korral.

8. Juurdepääsuõiguse haldus

8.1. Juurdepääsuõiguse reguleerimine

8.1.1. Ettevõttes tuleb kehtestada juurdepääsuõiguste reguleerimiseks poliitika või protseduur, mis hõlmab juurdepääsuõiguse elutsükli kõiki faase, sh kasutaja esialgset registreerimist, juurdepääsuõiguse muutmist ja kasutaja lõplikku väljaregistreerimist ehk kasutajaõiguste peatamist või katkestamist.

8.1.2. Juurdepääsuõiguse poliitika või protseduur peab määratlema kõikvõimalikud juurdepääsukohad: töökoha arvuti, andmesidevõrk, operatsioonisüsteemid, rakendused ja andmebaasid, infovarade mobiilne ja kaugjuurdepääs, ajutise ja välise kasutaja ligipääs infosüsteemile jm.

8.1.3. Kõik, kes kasutavad infovara, tuleb identifitseerida ja autoriseerida. Vastavalt infovara tundlikkuse tasemele tuleb kehtestada kasutajatele identifitseerimise ja autoriseerimise tase ning vastavad reeglid.

8.1.4. Juurdepääsuõigused ja muu töökorraldus tuleb reguleerida 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 tuvastatav iga toimingu osas.

8.1.5. Ettevõtte peab kehtestama ja rakendama juurdepääsuõiguste kontrolli protseduuri. Dokumenteeritud ja reaalselt väljastatud juurdepääsuõiguste vastavust tuleb regulaarselt kontrollida. Regulaarselt tuleb hinnata ka kasutajale antud õiguste vastavust tema tööalastele vajadustele. Kontrolli käigus tuvastatud juurdepääsuõigused, millel kasutaja puudub või ei ole asjakohane, tuleb eemaldada.

8.1.6. Juurdepääs andmetele ja informatsioonile tuleb piiritleda üksnes isikutega, kellele on seda oma tööülesannete täitmiseks vaja. Juurdepääsuõiguste andmine tuleb kooskõlastada infovara omanikuga. Eeltoodud nõue kehtib ka infosüsteemi nn tehniliste kasutajate osas.

Juurdepääsuõigused peavad olema dokumenteeritud ja põhinema infovara omaniku tahtel. Juurdepääsuõiguste dokumenteerimise meetod peab tagama ühese ja selge ülevaate juurdepääsuõiguste halduse protsessist ning kehtivatest juurdepääsuõigustest.

8.1.7. Töötajatelt ja välistelt teenusepakkujatelt tuleb töösuhte, lepingu või kokkuleppe lõppemisel võtta ära juurdepääsuõigused teabele ja infotöötlusvahenditele. Töösuhte, lepingu või kokkuleppe muutumisel tuleb juurdepääsuõiguseid vastavalt vajadusele kohandada. Erilist tähelepanu tuleb pöörata juurdepääsuõiguste õigeaegsele sulgemisele töötaja lahkumisel või teenusepakkujaga töösuhte lõpetamisel. Usalduse kaotuse puhul tuleb juurdepääsuõigused infosüsteemides sulgeda enne kui töötajale või välisele teenusepakkujale tehakse ametlikult teatavaks temaga sõlmitud lepingu lõpetamine. Töötaja pikema eemal viibimise korral tuleb kaaluda töötajale antud juurdepääsuõiguste peatamist eemal viibimise ajaks.

8.1.8. Unikaalsed kasutajatunnused tuleb määrata ka süsteemiadministraatoritele. Kui kasutatav tehnoloogia võimaldab, tuleb lisaks sisse-ehitatud administraatori kontole igapäevaste süsteemide haldusega seotud tegevuste jaoks luua individuaalsed kontod iga administraatori jaoks. Koopiaid administraatoriõigustega seotud ühiskasutatavatest koodidest ning paroolidest tuleb säilitada turvalisel viisil.

8.1.9. Administraatorite või privilegeeritud kontode osas tuleb rakendada rangemaid reegleid võrreldes tavakasutajate kontodega (sh nõuded autentimismeetmete kehtivusele ja keerukusele, toimingute logimine, ühiskasutatavate kontode autentimistunnuste muutmisprotseduur töötaja lahkumisel).

8.2. Autentimine

8.2.1. Ettevõttes peab kehtestama reeglid sobivate autentimismeetmete kasutamiseks (nt parool, PIN-kood, kiipkaart, biomeetrilised pääsumeetmed, jne).

8.2.2. Ettevõtte sisevõrgu infosüsteemi teenuste kasutamist väljastpoolt tuleb erilise hoolega jälgida. Enne kaugligipääsu teenuse avamist ja vastava ligipääsuõiguse andmist tuleb tuvastada välise kasutaja identiteet ja autentsus konkreetse teenuse kasutamiseks ning vastavate toimingute tegemiseks. Vastavalt teenuse iseloomule tuleb kaaluda sellise teenuse kasutajate puhul multiautentimise lahendust.

8.2.3. Salasõnade haldus tuleb kooskõlastada organisatsiooni infovara omanikega ja see peab olema kõigile infovarale juurdepääsu omavatele töötajatele teada. Salasõnade haldus 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.

8.2.4. Ettevõte peab kehtestama 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.

8.2.5. Salajane autentimisteave tuleb hoida konfidentsiaalsena. Ühtlasi tuleb tagada, et salajane autentimisteave ei saa teistele töötajatele või kolmandatele isikutele teatavaks (nt paroole tohib säilitada ainult krüpteeritud kujul, üksikkasutaja salasõna ei tohi ühiselt kasutada).

8.2.6. Kasutajaid tuleb teavitada nende kohustusest salasõnade turvalisel kasutamisel. Infosüsteemis tehtud toimingute eest on vastutav kasutaja, kellele salasõnaga ligipääs infosüsteemile saadakse.

9. Süsteemide arendus ja hankimine

9.1.1. IT lahenduse väljatöötamisel või hankimisel on vaja spetsifitseerida lahenduse funktsionaalsed ja mittefunktsionaalsed nõuded, sh hooldatavus, jõudlus, töökindlus, seire, turvalisus ja ühilduvus olemasolevate süsteemidega.

9.1.2. Infosüsteemi arendamine peab lähtuma ettevõtte vajadustest. Otsuse arendusprojektide käivitamise kohta peab tegema juhtkond tuginedes kinnitatud IT strateegiale.

9.1.3. Ettevõtte ärinõuete täitmiseks sobiva lahenduse loomiseks või hankimiseks peab esmalt välja selgitama vastavad kasutaja nõuded ning hindama alternatiivseid lahendusi. Juhtkond peab tegema otsuse arendusprojekti alustamise kohta ning alternatiivsete lahendusete puhul valiku tegemisel tuginema teostatavusanalüüsile, milles on näidatud ära projekti tehniline, operatsiooniline ning majanduslik põhjendatus.

9.1.4. Ettevõte peab tagama süsteemiarenduse ja -muudatuste halduse protsesside korrektse toimimise, et minimiseerida turvariske nii uute lahenduste osas kui nendega seotud olemasolevate lahenduste osas.

9.1.5. Ettevõtte infosüsteemide arendamisel, muutmisel ja täiendamisel peavad infosüsteemid töötlema infot ettenähtud korras. Andmekvaliteedi tagamist peavad toetama kontrollid nii andmete sisestamisel kui väljundi kasutamisel.

9.1.6. Infosüsteemi juurutamine ei tohi negatiivselt mõjutada ettevõtte olemasolevat infrastruktuuri ja teiste samas infrastruktuuris toimivate süsteemide turvalisust.

9.1.7. Tarkvara rakenduste arendamisel tuleb kasutada parimaid teadaolevaid praktikaid ja järgida infoturbe tagamise põhimõtteid kogu tarkvaraarenduse elutsükli jooksul.

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

9.1.9. Süsteeminõuded, standardid, vastuvõtukriteeriumid ning intellektuaalse omandi õigused tuleb fikseerida arendustööde tellimisel välistelt teenusepakkujatelt.

9.1.10. Selgelt tuleb määratleda testimisstandardid ning süsteemi vastuvõtukriteeriumid. Enne infosüsteemi juurutamist peab läbi viima süsteemi testimise vastavalt testimisplaanile. Testimisplaan peab sisaldama muu hulgas ka turvalisuse ning liidestatud süsteemide teste.

9.1.11. Testkeskkonnas peaks vältima reaalsete andmete kasutamist. Juhul kui kasutatakse arenduse- või testkeskkonnas tegelikke andmeid, tuleb neile keskkondadele rakendada tootmiskeskkonnaga võrdseid turvameetmeid (sh õiguste andmine, autentimine ja auditeerimise protseduurid, logimine).

10. Intsidentide haldus

10.1. Intsidentide haldus

10.1.1. Turvarünnetest, avariidest ja tõrgetest tingitud kahjude vähendamiseks, intsidentide registreerimiseks, neile reageerimiseks ning vastavate järelduste tegemiseks peab ettevõte kehtestama protseduurid ning töökohustused.

10.1.2. Teavitamisprotseduur eri tüüpi intsidentide (nt infoturbe rikkumine, oht, defekt või tõrge), mis võivad mõjutada ettevõtte varade turvalisust, tuleb teatavaks teha kõigile asjaomastele osapooltele. Igast avastatud või kahtlustatavast intsidentidest tuleb teavitada nii kiiresti kui võimalik.

10.1.3. Intsidendi lahendamisel tuleb säilitada intsidendi lahendamise käigus saadud informatsioon, 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.

10.1.4. Ettevõtte protseduurireeglid peavad tagama, et igale tuvastatud ja raporteeritud intsidendile määratakse vastutaja, kelle peamiseks eesmärgiks on intsidendi lahendamise koordineerimine. Protseduurireeglid peavad muuhulgas sisaldama intsidendi potentsiaalse eskaleerumise kirjeldust.

10.1.5. Intsidente tuleb analüüsida, et välja selgitada nende põhjused, tuvastada võimalikud puudused ja välja töötada meetmed (hinnata varsemalt rakendatud meetmete efektiivsust) puuduste likvideerimiseks vältides seeläbi sarnaste intsidentide kordumist tulevikus. Intsidentide analüüsimine aitab ühtlasi hinnata rakendatud meetmete efektiivsust ning 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.

10.2. Intsidentidest teavitamine

10.2.1. Finantsjärelevalve subjektide tegevust reguleerivad õigusaktid sätestavad Finantsinspektsiooni õiguse saada finantsjärelevalve subjektilt järelevalve teostamiseks teavet.

10.2.2. Tuginedes Juhendi punktis 10.2.1 sätestatule palub Finantsinspektsioon, et ettevõte:

10.2.2.1. teavitaks esimesel võimalusel Finantsinspektsiooni olulistest intsidentidest, edastades intsidendi osas nii palju infot, kui teavitamise hetkel võimalik.

10.2.2.2. hiljemalt kolm tööpäeva pärast olulise intsidendi lahendamist tuleb Finantsinspektsioonile esitada toimunu kirjeldus, kasutades üldiseid kontaktandmeid ja tuues ära järgmised andmed:

- intsidendi tüüp (käideldavus, terviklus, konfidentsiaalsus);
- intsidendi toimumise aeg;
- intsidendi ulatus ja mõju;
- intsidendi kirjeldus;
- intsidendi põhjus;
- intsidendi lahendus;
- meetmed, mida kavatsetakse rakendada tulevikus sarnaste juhtumite ärahoidmiseks.

10.2.3. Kui järelevalvesubjekt edastab punktis 10.2.2 kirjeldatud informatsiooni Finantsinspektsioonile mõne õigusakti alusel toimiva raporteerimise raames, loetakse punktis 10.2.2 kirjeldatud teavituskohustus täidetuks.

11. Infotehnoloogia ja infoturbe korralduse kontroll ja hindamine

11.1.1. Ettevõttes tuleb kehtestada nõuded infotehnoloogia ja infoturbe korralduse regulaarseks ja oluliste muudatuste korral erakorraliseks kontrolliks ja hindamiseks. Hinnata tuleb, kas infotehnoloogia ja infoturbe korralduses on järgitud ettevõtte siseselt kehtestatud nõudeid, IT teenuste tõhusust ja IT tegevuse vastavust ärilistele eesmärkidele.

11.1.2. Infotehnoloogia ja infoturbe korralduse juhtimismehhanismide, asjakohastele õigusaktide ja eeskirjade vastavuse, lepinguliste kohustuste täitmise ja rakendatud tehniliste meetmete hindamiseks tuleb vajadusel kasutada asjassepuutuvas valdkonnas sõltumatut osapoolt, näiteks siseauditi meeskond, vajadusel välist audiitorit. Hindamise tulemused esitatakse ettevõtte juhtkonnale, kes puuduste korral rakendab korrigeerivad meetmed.

11.1.3. Infotehnoloogia ja infoturbe korraldusega seotud auditite vajaduse tuvastamisel ja auditite planeerimisel tuleb vastava oskusteabe puudumisel kaaluda IT auditite läbiviimise teenuse edasiandmist. Otsustades auditi läbiviimise välise teenuspakkujaga, tuleb hinnata teenusepakkuja kompetentsi ning kogemust sarnaste auditite läbiviimisel.

11.1.4. Ettevõtte infotehnoloogia ja infoturbe korralduse juhtimisel ja planeerimisel tuleb võtta arvesse auditi tähelepanekuid ja märkusi. Kui auditi käigus avastatakse tõsisemaid puudusi ettevõtte infotehnoloogia ja infoturbe korralduses, tuleb pärast puuduste kõrvaldamist teostada järelaudit.

11.1.5. Võimalike nõrkuste väljaselgitamiseks kriitilistes infosüsteemides tuleb põhjaliku auditi teostamise kõrval kaaluda ründetestide (penetration testing) läbiviimist. Ründetestide läbiviimisel peab olema tagatud, et ettevõtte normaalne töö ei saaks häirida ega ettevõtte tööalane informatsioon kahjustada.

11.1.6. Ettevõtte juhtkond peab tagama regulaarse infotehnoloogia ja infoturbe korralduse vastavuse hindamise välistele nõuetele (seadused, regulatsioonid, lepingud jmt) ning nende mõjudega arvestamise. Vajadusel tuleb rakendada meetmeid infotehnoloogia ja infoturbe korralduse vastavusse viimiseks väliste nõuetega. Kõik kohaldatavad õigusaktide, eeskirjade ja lepingute nõuded ning organisatsiooni meetod nende nõuete täitmiseks tuleks iga infosüsteemi ja kogu organisatsiooni kohta selgelt piiritleda, dokumenteerida ja ajakohasena hoida. Ettevõttes tuleb rakendada asjakohaseid protseduure, et tagada vastavus õigusaktide, eeskirjade ja lepingute ning põhitegevuse nõuetega, mis puudutavad intellektuaalse omandi õigusi (sh nt omandlike tarkvaratoodete kasutamist), andmestike kaitset (nt kaotsimineku, hävituse, võltsimise, volitamata juurdepääsu ja volitamata avaldamise eest), privaatsuse ja isikutuvastusteabe kaitset ning krüptograafilisi turvameetmete kasutamist.

12. Rakendamine

Juhend käesolevas redaktsioonis jõustub alates 30.06.2020.