Sisukord

Infoturbe kohaldusmäärang

Kinnitatud: 20.10.2021

- Selle jaotise viitetabel näitab, kuidas Directo kontrollieesmärgid kohalduvad standardi praeguse versiooni ISO/IEC 27001:2013 nõuetega. Selle standardi täpse informatiooni leiate aadressilt http://www.iso.org.
- Antud dokument ühildub ISO/IEC27001:2013 turvapoliitika lisa/Annex A nõuetega.

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.5	INFOTURVAPOLIITIKA		
A.5.1	JUHTIMISSUUND INFOTURBE JAOKS		
A.5.1.1.	Infoturvapoliitika	Tuleb koostada juhtkonna poolt infoturbepoliitika ja see töötajatele mõistetavaks teha ja ka asjassepuutuvatele välistele pooltele.	JAH
A.5.1.2	Infoturvapoliitika ülevaatus	Vajalik perioodiliti või muutuste korral infoturbepoliitika üle vaadata.	JAH
A.6	INFOTURBE KORRALDUS		
A.6.1	SISEMINE INFOTURBE KORRALDUS		
A.6.1.1	Rollid ja kohustused infoturbe alal	Tuleb määratleda ja jaotada kõik kohustused infoturbe alal.	JAH
A.6.1.2	Kohustused ja lahusus	Organisatsiooni varade lubamatu või ettekavatsematu muutmise või väärkasutuse võimaluse vähendamiseks tuleb vastuolus olevad töökohustused ja vastutusalad lahutada.	JAH
A.6.1.3	Kontakt ametivõimudega	Tuleb olla asjakohaselt ühenduses asjaomaste ametivõimudega.	JAH
A.6.1.4	Kontakt erihuvigruppidega	Tuleb olla asjakohaselt ühenduses asjaomaste erialagruppidega või muude erialaste turvafoorumite ja erialaühingutega.	JAH
A.6.1.5	Infoturve projektijuhtimises	Sõltumatult projekti tüübist tuleb infoturvet projektijuhtimises arvestada.	JAH
A.6.2	Mobiilseadmed ja kaugtöö		
A.6.2.1	Mobiilseadmete kasutamise poliitika	Mobiilseadmete kasutamisega seotud riskide haldamiseks tuleb rakendada vastavat poliitikat ja seda toetavaid turvameetmeid.	JAH
A.6.2.2	Kaugtöö	Kaugtöökohtadel võetava, töödeldava või talletava teabe kaitseks tuleb rakendada vastavat poliitikat ja seda toetavaid turvameetmeid.	JAH
A.7	INIMRESSURSITURVE		
A.7.1	ENNE TÖÖSUHET		
A.7.1.1	Taustakontroll	Kõigi töökohakandidaatide tausta tuleks kontrollida vastavalt kohalduvaile õigusaktidele, eeskirjadele ja eetikanormidele ning kontroll peab olema õiges proportsioonis tegevusalaste nõuete, kättesaadavaks tehtava teabe turvamäärangu ja tajutud riskidega.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.7.1.2	Töölepingu sätted	Töötajate ja alltöövõtjate sõlmitavad lepingud peavad sõnastama nende ja organisatsiooni kohustused infoturbe alal.	JAH
A.7.2	TÖÖSUHTE AJAL		
A.7.2.1	Juhtkonna kohustused	Juhtkond peab nõudma töötajatelt ja alltöövõtjailt infoturbe rakendamist vastavalt organisatsioonis kehtestatud poliitikatele ja protseduuridele.	JAH
A.7.2.2	Infotuvateadlikkus - haridus ja koolitus	Kõik organisatsiooni töötajad ning kohaldatavail juhtudel ka alltöövõtjad peavad saama oma tööülesannetele vastava asjakohase teadvustuskoolituse ja regulaarseid täiendusteavitusi organisatsiooni poliitikate ja protseduuride alal.	JAH
A.7.2.3	Distsiplinaarprotsess	Teabe turvalisust rikkunud töötajate korralekutsumiseks peaks olema kehtestatud formaalne ja teatavaks tehtud distsiplinaarprotsess.	JAH
A.7.3	TÖÖSUHTE LÕPETAMINE VÕI MUUTMINE		
A.7.3.1	Töökohustuste lõpetamine või muutmine	Tuleb määratleda infoturbekohustused, mis jäävad kehtima pärast töösuhte lõpetamist või muutmist, teha need töötajale või alltöövõtjaile teatavaks ja tagada nende täitmine.	JAH
A.8	VARADE HALDUS		
A.8.1	VASTUTUS VARADE EEST		
A.8.1.1	Varade inventariloend	Tuleb piiritleda teabe ning muud teabe ja infotööstusvahenditega seotud varad ning pidada nende varade inventariloendit.	JAH
A.8.1.2	Varade omanikud	Inventariloendisse kuuluvad varad peavad kajastama omanikke.	JAH
A.8.1.3	Varade lubatav kasutamine	Tuleb piiritleda, dokumenteerida teabe ja infotöötlusvahenditega seotud varade lubatava kasutamise reeglid.	JAH
A.8.1.4	Varade tagastamine	Kõik töötajad ja välised kasutajad peavad oma töösuhte, lepingu või kokkuleppe lõppemisel tagastama kõik nende valduses olevad organisatsiooni varad.	JAH
A.8.2	TEABE TURVALIIGITUS		
A.8.2.1	Teabe turvaliigitus	Teave tuleks liigitada, lähtudes õigusaktide nõuetest, väärtustest, elutähtsusest ja tundlikkusest lubamatu paljastamise või muutmise suhtes.	JAH
A.8.2.2	Teabe märgistamine	Tuleb väljatöötada ja sisse seada sobiv organisatsioonis rakendatavale teabe turvaliigituse skeemile vastav protseduuristik teabe märgistamiseks.	JAH
A.8.2.3	Varade käitlus	Tuleb väljatöötada ja sisse seada sobiv organisatsioonis rakendatavale teabe turvaliigituse skeemile vastav protseduuristik varade käitluseks.	JAH
A.8.3	INFOKANDJATE KÄITLUS JA EDASTUS		

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.8.3.1	Ird-infokandjate haldus	Välised infokandjaate (mälupulgad, kõvaketted jne) halduseks tuleb määratleda juhised	JAH
A.8.3.2	Infokanjate kõrvaldamine	Infokandjat, mida enam ei vajata tuleb formaalsete protseduuridega turvaliselt ja ohutult kõrvaldada	JAH
A.8.3.3	Füüsiliste infokandjate transport	Teavet sisaldav infokandja tuleb transportimisel kaitsta lubamatu väärkasutuse ja rikkumise eest.	JAH
A.9	PÄÄSU REGULEERIMINE		
A.9.1	TÖÖALANE VAJADUS PÄÄSU REGULEERIDA		
A.9.1.1	Pääsu reguleerimise poliitika	Tööalaste nõuete ja infoturvanõuete põhjal tuleb kehtestada dokumenteerida ja läbi vaadata pääsu reguleerimise poliitika.	JAH
A.9.1.2	Juurdepääs võrgule ja võrguteenustele	Kasutajatel võib olla juurdepääs ainult sellele võrgule ja neile võrguteenustele, mida neil on konkreetselt lubatud kasutada.	JAH
A.9.2	KASUTAJATE PÄÄSUVÕIME HALDUS		
A.9.2.1	Kasutajate registreerimine ja välja registreerimine	Pääsuõiguste andmiseks tuleb kehtestada formaalne kasutajate registreerimise ja väljaregistreerimise protsess.	JAH
A.9.2.2	Kasutajate pääsuõiguste andmine	Kõigile süsteemidele ja teenustele juurdepääsu andmiseks ja selle äravõtmiseks tuleks kasutajatüüpidele kehtestada formaalne kasutajate registreerimise ja väljaregistreerimise protseduur.	JAH
A.9.2.3	Eelis pääsuõiguste haldus	Eelis pääsuõiguste andmist ja kasutamist tuleb kitsendada ja reguleerida	JAH
A9.2.4	Kasutajate salajase audentimisteabe haldus	Salajase audentimisteabe jaotamist tuleb reguleerida formaalse haldusprotsessiga.	JAH
A.9.2.5	Kasutajate pääsuõiguste läbivaatus	Varade omanikud peavad regulaarsete vaheaegade järel vaatama läbi kasutajate pääsuõigused.	JAH
A.9.2.6	Pääsuõiguste äravõtmine või korrigeerimine	Kõigilt töötajatelt ja välistelt kasutajatelt tuleb nende töösuhte, lepingu lõpetamisel võtta teabele ja infotöötlusvahenditele juurdepääsu õigused. Töösuhte, lepingu või kokkuleppe muutmisel õigusi korrigeerida.	JAH
A.9.3	KASUTAJA KOHUSTUSED		
A.9.3.1	Salajase audentimisteabe kasutamine	Kasutajailt tuleb salajase autentimisteabe kasutamisel nõuda organisatsiooni tavade järgimist.	JAH
A.9.4	SÜSTEEMIDE JA RAKENDUSTE PÄÄSUDE REGULEERIMINE		
A.9.4.1	Teabepääsu kitsendamine	Juurdepääsu teabele ja rakendussüsteemide funktsioonidele tuleb kitsendada vastavalt pääsu reguleerimise poliitikale.	JAH
A.9.4.2	Turvalised sisseogimise protseduurid	Seal, kus seda nõuab pääsu reguleerimise poliitika tuleb juurdepääsu süsteemidele ja rakendustele reguleerida turvalise sisselogimisprotseduuridega.	JAH
A.9.4.3	Paroolihalduse protseduur	Süsteemid paroolide halduseks peavad olema interaktiivsed ja tagama kvaliteetseid paroole.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.9.4.4	Eelis- utiliitide kasutamine	Süsteemi ja rakenduse turvameetmetest mööduda suutvate utiliitide kasutamist tuleb kitsendada ja rangelt reguleerida.	JAH
A.9.4.5	Programmide lähtekoodi pääsu reguleerimine	Juurdepääs programmide lähtekoodile peab olema kitsendatud	JAH
A.10	KRÜPTOGRAAFIA		
A.10.1	KRÜPTOGRAAFILISED TURVAMEETMED		
A.10.1.1	Krüptograafiliste turvameetmete kasutamise poliitika	Teabe kaitseks tuleb välja töötada ja evitada krüptograafiliste turvameetmete kasutamise poliitika.	JAH
A.10.1.2	Võtmehaldus	Tuleb välja töötada krüptograafiliste kasutamise, kaitse ja eluea poliitika ning rakendada seda kogu nende elutsükli kestel.	JAH
A.11	FÜÜSILINE JA KESKKONNATURVE		
A.11.1	TURVALISED ALAD		
A.11.1.1	Füüsiline turvaperimeeter	Tundlikku või elutähtsat teavet ja infotöötlusvahendeid sisaldavate alade kaitseks tuleb määratleda ja kasutada turvaperimeetreid.	JAH
A.11.1.2	Füüsilise sissepääsu reguleerimise meetmed	Turvalisi alasid tuleb kaitsta sobivate sissepääsu reguleerimise meetmetega, mis tagavad, et sissepääs on ainult volitatud personalil.	JAH
A.11.1.3	Kabinettide, ruumide ja rajatiste turve	Tuleb kavandada kabinettide, ruumide ja rajatiste füüsiline turve ja seda rakendada.	JAH
A.11.1.4	Kaitse väliste ja keskkonnaohtude eest	Tuleb kavandada füüsiline kaitse loodusõnnetuste, kuritahtlike rünnete või õnnetuste eest ning seda rakendada.	JAH
A.11.1.5	Töötamine turvalistel aladel	Tuleb kavandada turvalistel aladel töötamise protseduurid ning neid rakendada.	JAH
A.11.1.6	Tarne ja laadimisalad	Tarne ja laadimisalad jms pääsukohti ning muid kohti, kus volitamata isikud võivad territooriumile siseneda, tuleb lubamatu juurdepääsu vältimiseks reguleerida ning võimaluse korral isoleerida infotöötlusvahenditest.	EI
A.11.2	SEADMED		
A.11.2.1	Seadmete paigutus ja kaitse	Keskkonnaohtudest tulenevate ja lubamatu juurdepääsu võimaluste vähendamiseks tuleb seadmed sobivalt paigutada ja neid kaitsta.	JAH
A.11.2.2	Tehnilised tugiteenused	Seadmeid tuleb kaitsta või infoteenuseid toetavaid toite- ja sidekaableid tuleb kaitsta andmepüügi, häirete ja kahjustuste eest.	JAH
A.11.2.3	Kaabelduse turve	Andmeid kandvaid või infoteenust osutavaid toite ja sidekaableid tuleb kaitsta andmepüügi, häirete ja kahjustuste eest.	JAH
A.11.2.4	Seadmete hooldus	Seadmete pideva käideldavuse ja tervikluse tagamiseks tuleb neid õigesti hooldada.	JAH
A.11.2.5	Varade väljaviimine	Seadmeid, teavet ega tarkvara ei tohi eelneva loata territooriumilt välja viia.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.11.2.6	Seadmete ja varade turve väljaspool territooriumi	Väljapool territooriumi asuvatele varadele tuleb rakendada turvet, mis arvestatakse mitmesuguseid väljapool organisatsiooni territooriumi töötamise riske.	JAH
A.11.2.7	Seadmete turvaline kõrvaldamine või taaskasutus	Kõiki salvestuskandjat sisaldavaid seadmeüksusi tuleb enne nende kõrvaldamist või taaskasutust kontrollida veendumiseks, et kõik tundlikud andmed ja litsentsitarkvara on kõrvaldatud või turvaliselt üle kirjutatud.	JAH
A.11.2.8	Järelvalveta kasutajaseadmed	Kasutajad peavad tagama, et järelvalveta seadmetel on asjakohane kaitse.	JAH
A.11.2.9	Tühja laua ja tühja ekraani poliitika	Paberdokumentidele ja ird infokandjatele tuleb rakendada tühja laua poliitikat ning infotöötlusvahendite tühja ekraani poliitikat.	JAH
A.12	KÄITUSE TURVE		
A.12.1	KÄITUSPROTSEDUURID JA -KOHUSTUSED		
A.12.1.1	Dokumenteeritud käitusprotseduurid	Käitusprotseduurid tuleb dokumenteerida ja teha kättesaadavaks kõigile neid vajavaile kasutajaile.	JAH
A.12.1.2	Muutusehaldus	Infoturvet mõjutavaid organisatsiooni, äriprotsesside, infotöötlusvahendite ja süsteemide muutusi tuleb ohjata	JAH
A.12.1.3	Suutvuse haldus	Süsteemide vajaliku sooritusvõime tagamiseks tuleb seirata ja korrigeerida ressursikasutust ning prognoosida tulevasi suutvusevajadusi.	JAH
A.12.1.4	Arendus-, testimis- ja käituskeskkondade lahusus	Käituskeskkonna lubamatu kättesaadavuse või muutmise riskide vähendamiseks peavad arendus-, testimis- ja käituskeskkonnad olema üksteisest lahus.	JAH
A.12.2	KAITSE KAHJURVARA EEST		
A.12.2.1	Kahjurvara tõrje meetmed	Kaitseks kahjurkoodi eest tuleb rakendada avastamis,- vältimis- ja taastemeetmeid koos kasutajate asjakohase teadlikkusega.	JAH
A.12.3	VARUNDAMINE		
A.12.3.1	Teabe varundamine	Vastavalt kokkulepitud varunduspoliitikale tuleb regulaarselt teha teabe, tarkvara ja süsteemikujutise varukoopiaid ning neid testida.	JAH
A.12.4	LOGIMINE JA SEIRE		
A.12.4.1	Sündmuse logimine	Tuleb luua sündmuslogid, mis jäädvustavad kasutajate toiminguid, tõrkeid ja infoturvasündmusi ning hoida neid käigus ja regulaarselt läbi vaadata.	JAH
A.12.4.2	Logiteabe kaitse	Logimisvahendeid ja logiteavet tuleb kaitsta manipuleerimise ja lubamatu juurdepääsu eest.	JAH
A.12.4.3	Administraatori- ja operaatorilogid	Süsteemiadministraatori ja süsteemioperaatori toiminguid tuleb logida ning neid tuleb kaitsta ja regulaarselt läbi vaadata.	JAH
A.12.4.4	Kellade sünkroniseerimine	Kõigi organisatsioonis või turvadomeenis asuvate asjassepuutuvate infotöötlussüsteemide kellad tuleb sünkroniseerida mingi kokkulepitud etaloni allikaga.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.12.5	TÖÖTARKVARA OHJE		
A.12.5.1	Tarkvara installeerimine töösüsteemidele	Tuleb kehtestada protseduurid millega ohjata tarkvara installeerimist töösüsteemidele	JAH
A.12.6	TEHNILISTE NÕRKUSTE HALDUS		
A.12.6.1	Tehniliste nõrkuste haldus	Tuleb õigel ajal hankida teavet kasutusolevate infosüsteemide tehniliste nõrkuste kohta, hinnata organisatsiooni avatust sellistele nõrkustele ning rakendada sobivaid meetmeid nendega kaasneva riski käsitluseks.	JAH
A.12.6.2	Kitsendused tarkvara installeerimisele	Kasutajaile tuleb kehtestada tarkvara installeerimist korraldavad reeglid ning need ellu viia.	JAH
A.12.7	INFOSÜSTEEMIDE AUDITI KAALUTLUSED		
A.12.7.1	Infosüsteemide auditi turvameetmed	Täitlusprotsesside katkestuste minimeerimiseks tuleb töösüsteemide kontrollimist sisaldavad auditi nõuded ja toimingud hoolikalt plaanida ja kokku leppida.	JAH
A.13	SIDE TURVE		
A.13.1	VÕRGUTURBE MEETMED		
A.13.1.1	Võrguturbe meetmed	Süsteemides ja rakendustes oleva teabe kaitseks tuleb võrke hallata ja reguleerida.	JAH
A.13.1.2	Võrguteenuste turve	Tuleb piiritleda ja võtta kõigisse võrguteenuse lepetesse turva mehhanismid, teenusetasemed ja haldusmeetmed, sõltumata sellest kas teenused saadakse organisatsioonist endast või tellitakse väljast.	JAH
A.13.1.3	Eraldamine võrkudest	Võrkudes tuleb eraldada infoteenuste, kasutajate ja infosüsteemide grupid	JAH
A.13.2	TEABE EDASTUSE KORD		
A.13.2.1	Teabe edastuse poliitikad ja protseduurid	Igat tüüpi sidevahendite kaudu sooritatava teabe edastuse kaitseks tuleb kehtestada formaalsed edastuse poliitikad, protseduurid ja turvameetmed.	JAH
A.13.2.2	Teabe edastamise lepped	Tegevusalase teabe edestamiseks organisatsiooni ja väliste poolte vahel tuleb sõlmida lepped.	JAH
A.13.2.3	Elektrooniline sõnumivahetus	Elektroonilises sõnumivahetuses sisalduv teave peab olema asjakohaselt käsitletud.	JAH
A.13.2.4	Konfidentsiaalsus ja mitte avalikustamislepped	Organisatsiooni teabekaitsevajadusi kajastavad nõuded konfidentsiaalsus ja mitteavalikustamislepetele tuleb piiritleda ja neid regulaarselt läbi vaadata.	JAH
A.14	SÜSTEEMIDE HANKIMINE, VÄLJATÖÖTAMINE JA HOOLDUS		
A.14.1	INFOSÜSTEEMIDE TURVANÕUDED		
A.14.1.1	Infoturvanõuete analüüs ja spetsifitseerimine	Uutele infosüsteemidele või olemasolevate infosüsteemide täiustustele esitatavate nõuete hulka tuleb võtta teabe turvalisusega seotud nõuded.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.14.1.2	Rakendusteenuste turve avalikes võrkudes	Avalikke võrke läbivates rakendusteenustes tuleb kaitsta pettuse, vaidluse ning lubamatu paljastamise ja muutmise eest.	JAH
A.14.1.3	Rakendusteenuste tehingute kaitse	Rakendusteenuste tehingutes sisaldavat teavet tuleb kaitsta pooliku edastuse, väärmarsruutimise, sõnumite lubamatu muutmise, lubamatu paljastuse, sõnumite lubamatu dubleerimise või taasesituse eest.	JAH
A.14.2	TURVE ARENDUS- JA ABIPROTSESSIDES		
A.14.2.1	Turvalise arenduse poliitika	Tuleb kehtestada tarkvara ja süsteemiarenduse eeskirjad ning kohaldada neid arendustöödele organisatsioonis.	JAH
A.14.2.2	Süsteemi muudatuste ohje protseduur	Süsteemide muudatusi arenduse elutsüklis tuleb ohjata formaalsete muudatuseohje protseduuridega.	JAH
A.14.2.3	Rakenduste tehniline läbivaatus pärast tööplatvormide muudatusi	Tööplatvormide muudatuste korral tuleb põhitegevuse jaoks elutähtsad rakendused läbivaadata ja neid testida veendumiseks, et muudatused ei avalda negatiivset mõju organisatsiooni tegevusele ega turvalisusele.	JAH
A.14.2.4	Tarkvarapakettide muudatuste kitsendused	Tarkvarapakettide muudatusi tuleb hoida ohje all ja piirata neid vajadusel ning reguleerida.	JAH
A.14.2.5	Turvalise süsteemitehnika põhimõtted	Tuleb kehtestada ja dokumenteerida turvaliste süsteemide tehnolahenduse põhimõtted ning neid käigus hoida ja kohaldada kõigile infosüsteemide teostamise püüetele.	JAH
A.14.2.6	Turvaline arenduskeskkond	Organisatsioonid peavad kogu süsteemiarenduse elutsüklit hõlmavate süsteemide arenduste ja integratsiooni tarbeks rajama turvalised arenduskeskkonnad ja neid asjakohaselt kaitsma.	JAH
A.14.2.7	Väljasttellitud arendustöö	Organisatsioon peab väljast tellitud süsteemiarendust valvama ja seirama.	EI
A.14.2.8	Süsteemi turvatestimine	Arenduse ajal tuleb sooritada turvafunktsioonide testimine	JAH
A.14.2.9	Süsteemi vastuvõtu testimine	Uute infosüsteemide, ajakohasuste ja uute versioonide tarbeks tuleb kehtestada vastuvõtutingimuste programmid ja nendega seotud kriteeriumid.	JAH
A.14.3	TESTIMINE JA TESTANDMED		
A.14.3.1	Testandmete kaitse	Testandmeid tuleb hoolikalt valida, kaitsta ja ohjata.	JAH
A.15	TARNIJASUHTED		
A.15.1	INFOTURVE TARRNIJATE SUHETES		
A.15.1.1	Tarnijasuhete infoturvapoliitika	Tarnijaga tuleb kokku leppida ja dokumenteerida infoturvanõuded nende riskide vähendamiseks, mis on seotud tarnija juurdepääsuga organisatsiooni varadele.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.15.1.2	Turvalisuse lülitamine tarnijalepetesse	Tuleb kehtestada asjassepuutuvad infoturvanõuded ning leppida need kokku iga tarnijaga, kes pääseb organisatsiooni teabe juurde, võib seda töödelda või luua selle tarbeks IT taristu komponente.	JAH
A.15.1.3	Info- ja sidetehnoloogia tarneahel	Lepped tarnijatega peavad sisaldama nõudeid niisuguste infoturvariskide käsitlemiseks, mis seotud info- ja sidetehnolooogia teenuste ja toodete tarneahelaga.	JAH
A.15.2	TARNIJATE TEENUSTARNETE HALDUS		
A.15.2.1	Tarnijateenuste seire ja läbivaatus	Organisatsioonid peavad tarnijateenuste tarnimist regulaarselt seirama, läbi vaatama ja auditeerima	JAH
A.15.2.2	Tarnijateenuste muudatuste haldus	Muudatusi tarnijatelt teenuste saamises, sealhulgas seniste infoturvapoliitikate, protseduuride ja meetmete käigushoius ja täiustamises, tuleb hallata, arvestades asjassepuutuva talitusteabe ning töösüsteemide ja protsesside elutähtsust ning riskide ümberhindamist.	JAH
A.16	INFOTURVAINTSIDENTIDE HALDUS		
A.16.1	INFOTURBEINTSIDENTIDE HALDAMINE JA TÄIUSTUSED		
A.16.1.1	Kohustused ja protseduurid	Kiire, toimiva ja korrakohase infoturveintsidentide reageerimise tagamiseks tuleb kehtestada halduskohustused ja protseduurid.	JAH
A.16.1.2	Infoturvasündmusest teavitamine	Infoturvasündmustest tuleks teatada asjakohaste halduskanalite kaudu nii kiiresti kui võimalik.	JAH
A.16.1.3	Infoturvanõrkusest teatamine	Organisatsiooni infosüsteeme ja teenuseid kasutavailt töötajailt ja alltöövõtjailt tuleb nõuda, et nad paneksid tähele süsteemide või teenuste nõrkusi ning teataks kõigist ilmingutest või nõrkustest.	JAH
A.16.1.4	Infoturvasündmuste hindamine ja nende üle otsustamine	Infoturvasündmusi tuleks hinnata ja otsustada, kas nad tuleb liigitada infoturvaintsidentideks	JAH
A.16.1.5	Infoturvaintsidentide registreerimine	Infoturvaintsidentidele tuleb reageerida dokumenteeritud protseduuride kohaselt.	JAH
A.16.1.6	Infoturvaintsidentidest õppimine	Infoturvaintsidentide analüüsimine ja lahendusega saadud teavet tuleb kasutada tulevaste intsidentide võimalikkuse või toime vähendamiseks.	JAH
A.16.1.7	Asitõendite kogumine	Organisatsioon peab määratlema protseduurid asitõenditeks kõlbava teabe tuvastamiseks, kogumiseks, hankimiseks ja säilitamiseks ning neid protseduure rakendama.	JAH
A.17	JÄTKUSUUTLIKKUSE HALDUSE INFOTURBEASPEKTID		
A.17.1	INFOTURBE JÄRJEPIDEVUS		
A.17.1.1	Infoturbe jätkusuutlikkuse plaanimine	Organisatsioon peab määrama oma nõuded turvalisusele ja infoturbe halduse jätkusuutlikkusele ebasoodsates olukordades, näiteks kriisi või katastroofi ajal.	JAH

Kood	Tegevus	Meede	Kohaldub ettevõttes
A.17.1.2	Infoturbe jätkusuutlikkuse elluviimine	Organisatsioon peab kehtestama, dokumenteerima ja ellu viima protsessid, millega tagada infoturbe jätkusuutlikkuse nõutav tase ebasoodsates olukordades ning neid käigus hoidma.	JAH
A.17.1.3	Infoturbe jätkusuutlikkuse kontrollimine, läbivaatus ja hindamine	Organisatsioon peab kehtestatud ja rakendatud infoturbe jätkusuutlikkuse meetmeid regulaarsete vaheaegade järel kontrollima veendumiseks, et need on ebasoodsates olukordades kõlblikud ja toimivad.	JAH
A.17.2	DUBLEERIMINE		
A.17.2.1	Infotöötlusvahendite käideldavus	Infotöötlusvahendid tuleks evitada piisava dubleerimisega, et täita käideldavusnõudeid	JAH
A.18	VASTAVUS JA SISEAUDITID		
A.18.1	VASTAVUS ÕIGUSAKTIDE JA LEPINGUTE NÕUETELE		
A.18.1.1	Kohalduvate õigusaktide ja lepingunõuete väljaselgitamine	Kõik kohalduvad õigusaktide ja lepingute nõuded ning organisatsiooni meetod nende nõuete täitmiseks tuleb iga infosüsteemi ja organisatsiooni kohta selgelt piiritleda, dokumenteerida ja asjakohasena hoida.	JAH
A.18.1.2	Intellektuaalse omandi õigused	Tuleb rakendada asjakohaseid protseduure, millega tagada vastutus õigusaktide, eeskirjade ja lepingute ja põhitegevuse nõuetega.	JAH
A.18.1.3	Andmestike kaitse	Andmestikke tuleb tuleb kaitsta kaotsimineku, hävimise, võltsimise, lubamatu juurdepääsu, avaldamise eest vastavalt õigusaktide, eeskirjade ja lepinguliste kohustustega.	JAH
A.18.1.4	Privaatsus ja isikuandmete kaitse	Privaatsus ja isikuandmete kaitse tuleb asjakohastel juhtudel tagada vastavalt kohalduvatele õigusaktidele ja eeskirjadele.	JAH
A.18.1.5	Krüptograafiliste turvameetmete reguleerimine	Krüptograafilisi turvameetmeid tuleb kasutada kooskõlas kõigi kohalduvate lepete, õigusaktide ja eeskirjadega.	JAH
A.18.2	INFOTURBE LÄBIVAATUSED		
A.18.2.1	Infoturbe sõltumatu läbivaatus	Plaaniliste vaheaegade järel või oluliste muutatuste korral tuleb sõltumatult läbi vaadata organisatsiooni toimisviis infoturbe haldamisel ja teostamisel (poliitikad, protseduurid, eeskirjad)	JAH
A.18.2.2	Vastavus turvapoliitikale ja normidele	Juhid peavad oma vastutusalas regulaarselt läbi vaatama infotöötluse ja protseduuride vastavust asjakohastele turvapoliitikatele ja muudele nõuetele.	JAH
A.18.2.3	Tehnilise vastavuse läbivaatus	Regulaarselt tuleb kontrollida infosüsteemide vastavust organisatsiooni infoturbe juhtpõhimõtele ja normidele.	JAH