Sisukord

Infoturbe kohaldusmäärang 3

Infoturbe kohaldusmäärang

Kinnitatud: 09.09.2024

- Selle jaotise viitetabel näitab, kuidas Directo kontrollieesmärgid kohalduvad standardi praeguse versiooni ISO/IEC 27001:2022 nõuetega. Selle standardi täpse informatsiooni leiad aadressilt http://www.iso.org.
- Antud dokument ühildub ISO/IEC27001:2022 turvapoliitika lisa/Annex A nõuetega.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
5	Organisatsioon			
5.1	Infoturbe eeskirjad	Infoturbepoliitika ja teemapõhised poliitikad määratleb juhtkond, avaldatakse, edastatakse asjaomastele töötajatele ja asjaomastele huvitatud osapooltele ning neid tunnustatakse ja vaadatakse üle planeeritud ajavahemike järel ja oluliste muudatuste korral.	JAH	Ettevõtte infoturbesüsteemi loomisel on oluline järgida mitmeid põhimõtteid ning arvestada erinevate infoturbe aspektidega, et tagada ettevõtte andmete ja süsteemide turvalisus. Kirjeldame infoturbega seotud juhiseid, kuna see annab selged juhised ettevõtte infoturbenõuete täitmiseks.
5.2	Infoturbe rollid ja kohustused	Infoturbe rollid ja vastutusalad määratletakse ja jaotatakse vastavalt organisatsiooni vajadustele	JAH	Selged rollid ja kohustused, mis on kirjeldatud infoturbe käsiraamatu peatükis 5.2.
5.3	Tööülesannete lahusus	Puudub piisav kontroll ja vastutus.	JAH	Tuleks tagada, et pettusega ei oleks võimalik tegeleda. Ettevõttes peaks kogu süsteem ja sellega seotud protsessid olema kontrolli all.
5.4	Juhtimiskohustused	Juhtkond kehtestab infoturbe rakendamiseks selged rollid ja kohustused.	JAH	Ettevõttes on vaja näidata juhtkonna poolt pühendumust infoturbe juhtimissüsteemi vallas
5.5	Kontakt infoturbega seotud ametiasutustega	Organisatsioon loob ja hoiab kontakti asjaomaste asutustega.	JAH	Infoturbeintsidentidest tuleb teatada CERT-EE-le.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
5.6	Erihuvirühmadega (nt erialaliidud) ühendust võtmine	Organisatsioon loob ja hoiab kontakti erihuvirühmade või muude spetsialiseeritud turvafoorumite ja erialaliitudega	JAH	Hankige praegust infoturbeteavet infoturbe loenditest, foorumitest ja huvirühmadest.
5.7	Ohu luure	Infoturbeohtudega seotud teavet kogutakse ja analüüsitakse ohuteabe saamiseks.	JAH	Selleks, et olla valmis ja intsidente ennetada, peab olema info võimalike riskide ja nende vältimise meetodite kohta.
5.8	Infoturve projektijuhtimises	Infoturve on integreeritud projektijuhtimisse.	JAH	Projektide algatamisel tuleks arvestada infoturbe teemadega ja arvestada neid projekti käigus.
5.9	Teabe ja muude seotud varade inventuur	Teave ja muud varad tuleb sisestada SnipiT varade andmebaasi	JAH	Infovarade puudulik ülevaade võib põhjustada andmete terviklikkuse probleeme ning selleks tuleb hallata, millised infovarad ettevõttes olemas on.
5.10	Teabe ja muude seotud varade vastuvõetav kasutamine	Teabe ja muu seonduva vara vastuvõetava kasutamise reeglid ja kord tuleb kindlaks määrata, dokumenteerida ja rakendada.	JAH	Infokäsitlusreeglite puudumine võib põhjustada probleeme infovaradega ja turvaintsidente.
5.11	Varade tagastamine	Töötajad ja teised huvitatud isikud peavad töösuhte, lepingu või kokkuleppe muutmisel või lõpetamisel tagastama kogu nende valduses oleva organisatsiooni vara.	JAH	Tuleb jälgida, et varad oleksid ettevõtte poolt õigesti tasandatud.
5.12	Teabe klassifikatsioon	Teave klassifitseeritakse vastavalt organisatsiooni infoturbe vajadustele, lähtudes konfidentsiaalsusest, terviklikkusest, kättesaadavusest ja huvitatud osapoolte asjakohastest nõuetest.	JAH	Oluline on määratleda selged reeglid andmete konfidentsiaalseks hoidmiseks.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
5.13	Teabe märgistamine	Vastavalt organisatsiooni poolt vastu võetud teabe klassifitseerimisskeemile töötatakse välja ja rakendatakse teabe märgistamiseks sobiv protsess.	JAH	Teabe märgistamine on reegli täitmiseks oluline
5.14	Teabe edastamine	Suhtlemisreeglid, protseduurid või kokkulepped peavad olema paigas igat tüüpi suhtlusvahendite jaoks organisatsiooni sees ning organisatsiooni ja teiste osapoolte vahel	JAH	Kokkulepitud reeglistik aitab ära hoida infovarade edastamisega seotud intsidente.
5.15	Juurdepääsu kontroll	Teabele ja muule sellega seotud varale füüsilise ja loogilise juurdepääsu kontrollimise reeglid kehtestatakse ja rakendatakse äri- ja infoturbe nõuetest lähtuvalt.	JAH	Oluline on tagada õige juurdepääs õigetele andmetele.
5.16	Identiteedihaldus	Identiteedid hallatakse kogu teenuse/toote elutsükli jooksul	JAH	oluline on avastada identiteedi kadu või väärkasutus niipea kui võimalik
5.17	Autentimisteave	Protsessi käigus kontrollitakse autentimisinfo eraldamist ja haldamist, sealhulgas nõustatakse personali autentimisinfo nõuete täitmisel.	JAH	Tugeva parooli kasutamine peab olema kohustuslik kogu süsteemis. Lisaks paroolile tuleb rakendada mitmefaktoriline autentimine.
5.18	Juurdepääsuõigused	Juurdepääsuõigused teabele ja muudele seotud varadele antakse, vaadatakse üle, muudetakse ja eemaldatakse vastavalt organisatsiooni juurdepääsukontrolli poliitikatele ja reeglitele.	JAH	Juurdepääsuõigused tuleb anda õigele isikule, õigetel andmetel ja õigel ajal.
5.19	Infoturve tarnijasuhetes	Tarnija toodete või teenuste kasutamisega seotud infoturberiskide maandamiseks tuleb määratleda ja rakendada protsessid ja protseduurid.	JAH	Enne partneriks saamist tuleks läbi viia taustakontroll.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
5.20	Infoturbe käsitlemine tarnijalepingute raames	Asjakohased infoturbe nõuded kehtestatakse ja lepitakse kokku iga tarnijaga, lähtudes tarnijasuhte tüübist	JAH	Partnerluslepingusse tuleks lisada turvaklauslid.
5.21	Infoturbe haldamine info- ja kommunikatsioonitehnoloogia (IKT) tarneahelas	Protsessid määratletakse ja rakendatakse (IKT) tarneahela juhtimiseks	JAH	Enne partneriks saamist tuleks läbi viia taustakontroll.
5.22	Tarnijateenuste jälgimine, ülevaatamine ja muudatuste juhtimine	Organisatsioon jälgib, vaatab, hindab ja haldab regulaarselt tarnijate infoturbe praktikas ja teenuste osutamises toimunud muutusi.	JAH	Tagame, et tarnijad suudavad teenust pakkuda
5.23	Infoturve pilveteenuste kasutamisel	Pilveteenuste hankimise, kasutamise, haldamise ja väljumise protsessid on kehtestatud vastavalt organisatsiooni infoturbenõuetele	JAH	Enne teenusepakkujaks saamist tuleks läbi viia taustakontroll
5.24	Infoturbeintsidentide juhtimise planeerimine ja ettevalmistamine	Organisatsioon kavandab ja valmistub infoturbeintsidentide haldamiseks, määratledes, kehtestades ja teavitades infoturbeintsidentide haldusprotsesse, rolle ja vastutusi.	JAH	Juhtumeid on vaja õigesti juhtida ja käsitleda
5.25	Formeerimise turvasündmuste hindamine ja otsustamine	Organisatsioon hindab infoturbesündmusi ja otsustab, kas liigitada need infoturbeintsidentideks.	JAH	Teave intsidendi kohta tuleb võimalikult kiiresti esitada õigesti
5.26	Infoturbeintsidentidele reageerimine	Organisatsioon kavandab ja valmistab ette intsidentide haldamise töörühma	JAH	Organisatsioon kavandab ja valmistab ette intsidentide haldamise töörühma
5.27	Infoturbeintsidentidest õppimine	Infoturbeintsidentidest saadud teadmisi kasutatakse infoturbe kontrolli tugevdamiseks ja täiustamiseks	JAH	Juhtumi analüüsi tulemused ja rakendatud meetmed hoiavad ära kordumise
5.28	Tõendite kogumine	Organisatsioon kehtestab ja rakendab infoturbe sündmustega seotud tõendite tuvastamise, kogumise, hankimise ja säilitamise korra	JAH	Juhtumite analüüsimiseks on vaja koguda tõendeid

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
5.29	Infoturve häirete ajal	Organisatsioon peab planeerima, kuidas hoida infoturvet häirete ajal sobival tasemel.	JAH	Juhtumite ja häirete korral on võimalik tekitada lisakaja ja ära kasutada infoturbe nõrkusi.
5.30	IKT-valmidus talitluspidevuse tagamiseks	IKT valmiduse planeerimine, juurutamine, hooldamine ja testimine lähtub talitluspidevuse eesmärkidest ja IKT järjepidevuse nõuetest	JAH	Infosüsteemi arendamise aluseks peaks olema tegevuse järjepidevuse tagamine
5.31	Juriidilised, seadusandlikud, regulatiivsed ja lepingulised nõuded	Infoturbega seotud juriidilised, kohustuslikud, regulatiivsed ja lepingulised nõuded ning organisatsiooni lähenemisviis nende nõuete täitmiseks tuleb kindlaks teha, dokumenteerida ja ajakohastada	JAH	Infosüsteemid ja nende turvalisus peaksid vastama regulatiivsetele nõuetele ning arvestama huvitatud osapoolte nõuetega
5.32	Intellektuaalse omandi õigused	Organisatsioon rakendab intellektuaalomandi õiguste kaitsmiseks asjakohaseid protseduure.	JAH	Organisatsiooni intellektuaalomandit tuleks kaitsta
5.33	Kirjete kaitse	Dokumendid on kaitstud kaotsimineku, hävimise, võltsimise, volitamata juurdepääsu ja volitamata väljastamise eest	JAH	Oluline on kaitsta oma teabevarasid ja kaasnevaid andmeid.
5.34	Privaatsus ja isikut tuvastava teabe (PII) kaitse.	Organisatsioon tuvastab ja täidab privaatsuse kaitse nõudeid vastavalt kehtivatele seadustele ja määrustele ning lepingunõuetele	JAH	Kõik isikuandmetega seonduv peab olema kaitstud vastavalt GDPR nõuetele
5.35	Infoturbe sõltumatu ülevaade	Organisatsiooni lähenemine infoturbe juhtimisele ja selle juurutamine, sealhulgas inimesed, protsessid ja tehnoloogiad, vaadatakse planeeritud ajavahemike järel või oluliste muudatuste toimumisel iseseisvalt üle.	JAH	Sõltumatu organisatsioon peaks teabeturbe ja sellega kaasnevad nõuded regulaarselt üle vaatama.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
5.36	Infoturbe poliitikate, reeglite ja standardite järgimine	Korrapäraselt vaadatakse üle organisatsiooni infoturbepoliitika, kõrgeimate turvapõhiste poliitikate, reeglite ja standardite järgimine.	JAH	Infoturbesüsteem ja sellega kaasnevad nõuded tuleks regulaarselt üle vaadata. Läbivaatamisprotseduurid tuleks rakendada ja järgida.
5.37	Dokumenteeritud tööprotseduurid	Infotöötlusseadmete töökord dokumenteeritakse ja tehakse seda vajavale personalile kättesaadavaks.	JAH	Infoturbe tagamiseks on vaja kirjeldada tööprotsessi nõudeid
6	Töötajad			
6.1	Sõelumine	Kõigi kandidaatide taustakontroll viiakse läbi enne organisatsiooniga liitumist ja jooksvalt, võttes arvesse kehtivaid seadusi, määrusi ja eetikat ning see peab olema proportsionaalne ärinõuete, juurdepääsetava teabe konfidentsiaalsuse ja tajutavate riskidega.	JAH	Vajadus vältida motiveerimata ja mittepädevate töötajate värbamist
6.2	Töötingimused	Töölepingutes on määratletud personali ja organisatsiooni kohustused infoturbe valdkonnas.	JAH	Töötajad peavad olema motiveeritud täitma talle pandud ülesandeid ja saavutama tulemusi
6.3	Infoturbeteadlikkus, haridus ja koolitus	Organisatsiooni töötajad ja asjaomased sidusrühmad peavad saama vastavalt oma tööülesannetele asjakohast infoturbealast teadlikkust, koolitust ning korrapärase juurdepääsu organisatsiooni infoturbe poliitikatele ja protseduuridele.	JAH	Teadmatusest põhjustatud intsidente tuleb vältida.
6.4	Distsiplinaarprotsess	Infoturbepoliitika rikkumise toime pannud töötajate ja teiste huvitatud isikute suhtes algatatakse distsiplinaarmenetlus	JAH	Rikkumise korral on vaja kehtestada selged reeglid

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
6.5	Töösuhte lõppemise või muutumise järgsed kohustused	Võib esineda infoturbe kohustusi, mis jäävad kehtima ka pärast töösuhte lõppemist või muutumist. Nendest kohustustest tuleks teatada asjaomastele töötajatele ja teistele huvitatud isikutele.	JAH	Ettevõttes on vaja teada reegleid peale töösuhte
6.6	Konfidentsiaalsus- või mitteavaldamise lepingud	Konfidentsiaalsuslepingud, mis kajastavad organisatsiooni teabekaitse vajadusi, peaksid olema kindlaks tehtud, dokumenteeritud, korrapäraselt üle vaadatud ning töötajate ja teiste asjassepuutuvate sidusrühmade poolt allkirjastatud.	JAH	Reeglite täitmiseks on vaja kokku leppida tingimused ja nõuded
6.7	Kaugtöö	Kui töötajad töötavad eemalt, tuleb rakendada turvameetmeid, et kaitsta teavet, millele juurdepääs, mida töödeldakse või säilitatakse väljaspool organisatsiooni ruume.	JAH	Kodukontoris töötades on vaja kehtestada üheselt mõistetavad reeglid.
6.8	Infoturbe sündmuste aruandlus	Organisatsioon peab tagama töötajatele võimaluse õigeaegselt teavitada täheldatud või kahtlustatavatest infoturbesündmustest sobivate kanalite kaudu	JAH	Käsitleda tuleks juhtumeid, mis ei vasta infoturbesüsteemi nõuetele
7.	Füüsilised kontrollid			
7.1	Füüsilise turvalisuse perimeetrid	Füüsilised piirid on määratletud ja neid kasutatakse turvaalade ja ettevõtte varade kaitsmiseks	JAH	See tuleks kindlaks määrata ettevõtte füüsiline ümbermõõt ja märkida see selgelt.
7.2	Sissepääs turvaalale on kontrollitud	Turvaalade jaoks tuleks määratleda sisenemispunktid ja juurdepääsureeglid	JAH	Sisenemispunkte tuleb jälgida ja juurdepääsulogi peaks olema välja arvatud turvaliste alade jaoks
7.3	Kontorite, ruumide ja rajatiste turvamine	Kontorite, ruumide ja rajatiste füüsiline perimeeter on kindlustatud.	JAH	Tuleb rakendada füüsilisi abinõusid välistamaks kõrvaliste isikute sattumist turvaaladele.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
7.4	Füüsilise turvalisuse jälgimine	Ruumides tuleb pidevalt jälgida selleks volitatud isikuid	JAH	Vajalik korraldada turvaseire turvaaladel.
7.5	Kaitsmine füüsiliste ja keskkonnaohtude eest	Kavandage ja rakendage meetmeid füüsiliste ja keskkonnaohtude korral (looduskatastroofid, ebasobiv keskkond, füüsilised ohud)	JAH	Oluline on välja selgitada keskkonnaohud, nt voolukadu, tulekahjusignalisatsioon jne.
7.6	Juurdepääs turvalistele aladele	Turvaaladele juurdepääsureeglid on määratletud ja rakendatud	JAH	Määratletakse turvaalad ja neile juurdepääsureeglid.
7.7	Selge laud ja selge ekraan	Läbipaistva laua, printimise ja eemaldatava kandja ning selge ekraani reeglid; määratletakse ja jõustatakse teabetöötlusseadmete reeglid.	JAH	Andmelekke kohta on vaja kehtestada reeglid.
7.8	Seadmete paigutus ja kaitse	Seadmed peavad olema kindlas kohas ja kaitstud	JAH	Varustus vajab füüsilist kaitset ja reeglid tuleks vastavalt määratleda.
7.9	Varade turvalisus väljaspool äriruume	Väljaspool objekti asuv vara tuleb kaitsta.	JAH	Tuleks rakendada varade vastuvõetava kasutamise eeskirju.
7.10	Andmekandja	Säilituskandjaid hallatakse kogu nende soetamise, kasutamise, transportimise ja kõrvaldamise elutsükli jooksul vastavalt organisatsiooni klassifitseerimisskeemile ja käitlemisnõuetele.	JAH	Kolmandate isikute juurdepääs andmekandjatele võib põhjustada andmeleket. Ettevõttes on andmekandjatest juttu juhendi vastava peatüki all.
7.11	Kommunaalteenuste toetamine	Infotöötlusrajatised peavad olema kaitstud elektrikatkestuste ja muude tugiteenuste riketest põhjustatud häirete eest	JAH	Tööpidevuse tagamiseks tuleks kaaluda UPSi või alternatiivse toiteallika kasutamist.
7.12	Kaabli turvalisus	Toite-, andme- või tugiteabeteenuseid kandvad kaablid peavad olema pealtkuulamise, häirete või kahjustuste eest kaitstud	JAH	Vale kaabeldus võib põhjustada andmete kaaperdamist ja infoturbe intsidente.
7.13	Seadmete hooldus	Seadmeid tuleb korralikult hooldada, et tagada teabe kättesaadavus, terviklikkus ja konfidentsiaalsus	JAH	Seadmete hooldusnõuded on kirjeldatud infoturbe juhendis

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
7.14	Seadmete ohutu kõrvaldamine või taaskasutamine	Andmekandjaid sisaldavaid seadmeid kontrollitakse tagamaks, et tundlikud andmed ja litsentsitud tarkvara on enne kõrvaldamist või taaskasutamist eemaldatud või turvaliselt üle kirjutatud.	JAH	Ohtude tuvastamine on oluline enne kahju kuhjumist.
8.	Tehnoloogilised kontrollid			
8.1	Kasutaja lõpp-punkti seadmed	Kasutajaseadmete kaudu salvestatud, töödeldud või juurdepääsetav teave peab olema kaitstud.	JAH	Meede on vajalik meie rakenduse toimimiseks kliendi süsteemides.
8.2	Privilegeeritud juurdepääsuõigused	Privilegeeritud juurdepääsuõiguste eraldamine ja kasutamine on piiratud ja hallatud	JAH	Privilegeeritud juurdepääsuõiguste eraldamine ja kasutamine on piiratud
8.3	Andmetele juurdepääsu piirang	Juurdepääs andmetele ja nendega seotud varadele tuleb piirata vastavalt kehtestatud subjektipõhisele juurdepääsukontrolli poliitikale	JAH	Infole juurdepääsu reguleerimise protsessi on vaja käsitleda nii, et puudub volitamata juurdepääs ja andmed oleksid turvaliselt kaitstud.
8.4	Juurdepääs lähtekoodile	Lugemis- ja kirjutamisjuurdepääsu lähtekoodile, arendustööriistadele ja tarkvarateekidele tuleb asjakohaselt hallata.	JAH	Ligipääs lähtekoodile peab olema piiratud.
8.5	Turvaline autentimine	Turvalist autentimist rakendatakse teabe juurdepääsupiirangute ja juurdepääsu kontrollimise poliitikate alusel	JAH	Rakendage tugevate paroolide kasutamise eeskirju
8.6	Võimsuse juhtimine	Ressursikasutust jälgitakse ja kohandatakse lähtuvalt praegusest ja eeldatavast võimsusvajadusest.	JAH	Ressursivõimsust jälgitakse rakenduse ja süsteemide jõudluse osas.
8.7	Kaitse pahavara eest	Pahavaravastane kaitse peab olema rakendatud ja seda peab toetama asjakohane kasutajateadlikkus.	JAH	Vajalik kaitse pahavara eest

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
8.8	Tehniliste haavatavuste haldamine	Vaja on hankida teavet kasutusel olevate infosüsteemide tehniliste haavatavuste kohta, hinnata organisatsiooni kokkupuudet selliste haavatavustega ja võtta kasutusele asjakohased meetmed.	JAH	Valige kvaliteetsete seadmete ja hea tehnilise toega müüjad
8.9	Konfiguratsiooni juhtimine	Luuakse, dokumenteeritakse, rakendatakse, jälgitakse ja vaadatakse üle riistvara, tarkvara, teenuste ja võrkude konfiguratsioonid, sealhulgas turbekonfiguratsioonid.	JAH	Oluline on tagada, et kasutatakse õiget tarkvarakonfiguratsiooni.
8.10	Teabe kustutamine	Infosüsteemides, seadmetes või muudel andmekandjatel salvestatud teave kustutatakse, kui seda enam ei vajata	JAH	Meede, mis on vajalik andmete juhusliku lekke vältimiseks
8.11	Andmete maskeerimine	Andmete maskeerimist kasutatakse vastavalt organisatsiooni subjektipõhisele juurdepääsukontrolli poliitikale ja muudele seotud teemapõhistele põhimõtetele ja ärinõuetele, võttes arvesse kehtivaid seadusi.	JAH	Vajalikud andmed muudetakse anonüümseks.
8.12	Andmelekke vältimine	Andmelekke vältimise meetmeid rakendatakse süsteemide, võrkude ja muude seadmete puhul, mis töötlevad, salvestavad või edastavad tundlikku teavet	JAH	Andmetele juurdepääsu piiramiseks on vaja käsitleda protsesse.
8.13	Teabe varundamine	Teabe, tarkvara ja süsteemide varukoopiaid tuleb hooldada ja regulaarselt testida vastavalt kokkulepitud teemapõhisele varunduspoliitikale	JAH	Andmed, konfiguratsioonid, virtuaalsed masinate keskkonnad Varundab kiire jõudluse taastamiseks vajalikke andmeid
8.14	Infotöötlusseadmete koondamine	Teabetöötlusrajatised on rakendatud piisava koondamisega, et vastata kättesaadavusnõuetele.	JAH	Kättesaadavusnõuete täitmiseks on vaja rakendada koondamist.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
8.15	Logimine	Luuakse, hooldatakse, kaitstakse ja analüüsitakse logisid, mis salvestavad tegevusi, erandeid, vigu ja muid asjakohaseid sündmusi.	JAH	Logiserver tuleb juurutada ja seadmed logide saatmiseks konfigureerida
8.16	Seiretegevused	Võrke, süsteeme ja rakendusi jälgitakse ebatavalise käitumise suhtes ning rakendatakse asjakohaseid meetmeid võimalike infoturbeintsidentide hindamiseks	JAH	Infoturbesüsteemide terviklikkuse tagamiseks tuleks määratleda vajalik järelevalve.
8.17	Kella sünkroonimine	Organisatsioonis kasutatavate infotöötlussüsteemide kellad peavad olema sünkroniseeritud ja kontrollitud.	JAH	Kellade sünkroniseerimise tagamine ja kontrollimine on vajalik süsteemide korrektseks toimimiseks ja juhtimisprotsesside läbiviimiseks.
8.18	Privilegeeritud utiliitprogrammide kasutamine	Süsteemi ja rakenduste juhtelemente segavate utiliitprogrammide kasutamine peab olema piiratud ja rangelt kontrollitud	JAH	Ettevõttes kasutatakse piiratud privilegeeritud kommunaalteenuseid.
8.19	Tarkvara installeerimine operatsioonisüsteemidesse	Rakendatakse protseduure ja meetmeid tarkvara installimise turvaliseks haldamiseks operatsioonisüsteemidesse	JAH	Täiendava tarkvara installimiseks on vaja luba
8.20	Võrkude turvalisus	Võrgud ja võrguseadmed peavad olema kaitstud, hallatud ja kontrollitud, et kaitsta süsteemides ja rakendustes sisalduvat teavet.	JAH	Võrgukaablid ja võrguseadmed on turvalises kohas lukustatud riiulites, neid jälgitakse ja hallatakse turvalisel viisil.
8.21	Võrguteenuste turvalisus	Tuvastatakse, rakendatakse ja jälgitakse võrguteenuste turvamehhanisme, teenusetasemeid ja teenusenõudeid	JAH	Kasutatavad võrguteenused peavad olema kaitstud
8.22	Võrkude eraldamine	Infoteenuste, kasutajate ja infosüsteemide rühmad peavad olema organisatsiooni võrkudes eraldatud.	JAH	Vältida tuleks erinevate turvakeskkondade otseühendust võrgus

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
8.23	Veebi filtreerimine	Juurdepääsu välistele veebisaitidele hallatakse pahatahtliku sisuga kokkupuute minimeerimiseks.	JAH	Veebipõhine veebifiltreerimine tuleks rakendada, et pahatahtlikud veebisaidid automaatselt blokeerida.
8.24	Krüptograafia kasutamine	Määratletakse ja rakendatakse krüptograafia tõhusa kasutamise reeglid, sealhulgas krüptograafilise võtme haldamise reeglid	JAH	Vajalik konfidentsiaalsete andmete lekke vältimiseks
8.25	Turvaline arenduse elutsükkel	Kehtestatakse ja rakendatakse reeglid tarkvara ja süsteemide ohutuks arendamiseks.	JAH	Süsteemne turvalisus kogu rakenduse elutsükli jooksul
8.26	Rakenduse turvanõuded	Infoturbe nõuded tuvastatakse, täpsustatakse ja kinnitatakse rakenduse arendamise või hanke käigus.	JAH	Rakenduse arendamise ja täiustamise etapis on oluline jälgida turvaaspekte
8.27	Turvaline süsteemi arhitektuur ja põhimõtted	Turvaliste süsteemide kujundamise põhimõtted kehtestatakse, dokumenteeritakse, hooldatakse ja rakendatakse kõigis infosüsteemide arendustegevustes.	JAH	Arendustegevuse dokument peaks hõlmama turvalise arhitektuuri põhimõtteid
8.28	Turvaline kodeerimine	Tarkvaraarenduses rakendatakse turvalise kodeerimise põhimõtteid	JAH	Juhend turvaliseks arendustegevuseks.
8.29	Turvatestimine arenduses ja vastuvõtmisel	Turvatestimise protsessid määratletakse ja rakendatakse kogu arenduse elutsükli jooksul	JAH	Meie arendusprotsessi lahutamatu osa on testimine.
8.30	Väljastpoolt tellitud arendus	Organisatsioon juhib, jälgib ja vaatab üle sisseostetava süsteemiarendusega seotud tegevusi.	EI	Ettevõte ei kasuta tarkvara arendamiseks väliseid partnereid.
8.31	Arendus- ja testkeskkondade eraldamine	Arendus-, testi- ja kasutuskeskkonnad peavad olema eraldatud ja kaitstud.	JAH	Arendus ja testikeskkonnad peavad olema eraldatud, et kliendikeskkonda ei mõjutataks.
8.32	Muutuste juhtimine	Infotöötlusvahendite ja infosüsteemide muudatustele kohaldatakse muudatuste haldamise korda.	JAH	Tuleb tagada süsteemsed muudatused süsteemis, et muudatuste käsitlemisel ei tekiks turvaintsidente.

Kood	Kontrollid	Meede	Kohaldub JAH/EI	Meetme rakendamise vajadus või välistamise põhjendus
8.33	Testi andmed	Testiandmed peavad olema õigesti valitud, kaitstud ja hallatud	JAH	Testiandmed tuleks enne nende kasutamist ette valmistada (maskeerida).
8.34	Infosüsteemide kaitse auditi testimise ajal	Auditeerimistestid ja muud operatsioonisüsteemide hindamist hõlmavad tegevused planeeritakse ja lepitakse testija ja ettevõtte vahel kokku	JAH	Turvatestide protsess ja tingimused peavad olema süsteemselt ettevalmistatud.