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
5.	Organisatsioonilised kontrollid		
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
5.2	Infoturbe rollid ja kohustused	Infoturbe rollid ja vastutusalad määratletakse ja jaotatakse vastavalt organisatsiooni vajadustele	JAH
5.3	Tööülesannete lahusus	Puudub piisav kontroll ja vastutus.	JAH
5.4	Juhtimiskohustused	Juhtkond kehtestab infoturbe rakendamiseks selged rollid ja kohustused.	JAH
5.5	Kontakt infoturbega seotud ametiasutustega	Organisatsioon loob ja hoiab kontakti asjaomaste asutustega.	JAH
5.6	Erihuvirühmadega (nt erialaliidud) ühendust võtmine	Organisatsioon loob ja hoiab kontakti erihuvirühmade või muude spetsialiseeritud turvafoorumite ja erialaliitudega	JAH
5.7	Ohu luure	Infoturbeohtudega seotud teavet kogutakse ja analüüsitakse ohuteabe saamiseks.	JAH
5.8	Infoturve projektijuhtimises	Infoturve on integreeritud projektijuhtimisse.	JAH
5.9	Teabe ja muude seotud varade inventuur	Teave ja muud varad tuleb sisestada SnipiT varade andmebaasi	JAH
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
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
5.12	Teabe klassifikatsioon	Teave klassifitseeritakse vastavalt organisatsiooni infoturbe vajadustele, lähtudes konfidentsiaalsusest, terviklikkusest, kättesaadavusest ja huvitatud osapoolte asjakohastest nõuetest.	JAH
5.13	Teabe märgistamine	Vastavalt organisatsiooni poolt vastu võetud teabe klassifitseerimisskeemile töötatakse välja ja rakendatakse teabe märgistamiseks sobiv protsess.	JAH

Kood	Kontrollid	Meede	Kohaldub JAH/EI
5.14	Teabe edastamine	Suhtlemisreeglid, protseduurid või kokkulepped peavad olema paigas igat tüüpi suhtlusvahendite jaoks organisatsiooni sees ning organisatsiooni ja teiste osapoolte vahel	JAH
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
5.16	Identiteedihaldus	Identiteedid hallatakse kogu teenuse/toote elutsükli jooksul	JAH
5.17	Autentimisteave	Protsessi käigus kontrollitakse autentimisinfo eraldamist ja haldamist, sealhulgas nõustatakse personali autentimisinfo nõuete täitmisel.	JAH
5.18	Juurdepääsuõigused	Juurdepääsuõigused teabele ja muudele seotud varadele antakse, vaadatakse üle, muudetakse ja eemaldatakse vastavalt organisatsiooni juurdepääsukontrolli poliitikatele ja reeglitele.	JAH
5.19	Infoturve tarnijasuhetes	Tarnija toodete või teenuste kasutamisega seotud infoturberiskide maandamiseks tuleb määratleda ja rakendada protsessid ja protseduurid.	JAH
5.20	Infoturbe käsitlemine tarnijalepingute raames	Asjakohased infoturbe nõuded kehtestatakse ja lepitakse kokku iga tarnijaga, lähtudes tarnijasuhte tüübist	JAH
5.21	Infoturbe haldamine info- ja kommunikatsioonitehnoloogia (IKT) tarneahelas	Protsessid määratletakse ja rakendatakse (IKT) tarneahela juhtimiseks	JAH
5.22	Tarnijateenuste jälgimine, ülevaatamine ja muudatuste juhtimine	Organisatsioon jälgib, vaatab, hindab ja haldab regulaarselt tarnijate infoturbe praktikas ja teenuste osutamises toimunud muutusi.	JAH
5.23	Infoturve pilveteenuste kasutamisel	Pilveteenuste hankimise, kasutamise, haldamise ja väljumise protsessid on kehtestatud vastavalt organisatsiooni infoturbenõuetele	JAH
5.24	Infoturbeintsidentide juhtimise planeerimine ja ettevalmistamine	Organisatsioon kavandab ja valmistub infoturbeintsidentide haldamiseks, määratledes, kehtestades ja teavitades infoturbeintsidentide haldusprotsesse, rolle ja vastutusi.	JAH
5.25	Formeerimise turvasündmuste hindamine ja otsustamine	Organisatsioon hindab infoturbesündmusi ja otsustab, kas liigitada need infoturbeintsidentideks.	JAH
5.26	Infoturbeintsidentidele reageerimine	Organisatsioon kavandab ja valmistab ette intsidentide haldamise töörühma	JAH
5.27	Infoturbeintsidentidest õppimine	Infoturbeintsidentidest saadud teadmisi kasutatakse infoturbe kontrolli tugevdamiseks ja täiustamiseks	JAH

Kood	Kontrollid	Meede	Kohaldub JAH/EI
5.28	Tõendite kogumine	Organisatsioon kehtestab ja rakendab infoturbe sündmustega seotud tõendite tuvastamise, kogumise, hankimise ja säilitamise korra	JAH
5.29	Infoturve häirete ajal	Organisatsioon peab planeerima, kuidas hoida infoturvet häirete ajal sobival tasemel.	JAH
5.30	IKT-valmidus talitluspidevuse tagamiseks	IKT valmiduse planeerimine, juurutamine, hooldamine ja testimine lähtub talitluspidevuse eesmärkidest ja IKT järjepidevuse nõuetest	JAH
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
5.32	Intellektuaalse omandi õigused	Organisatsioon rakendab intellektuaalomandi õiguste kaitsmiseks asjakohaseid protseduure.	JAH
5.33	Kirjete kaitse	Dokumendid on kaitstud kaotsimineku, hävimise, võltsimise, volitamata juurdepääsu ja volitamata väljastamise eest	JAH
5.34	Privaatsus ja isikut tuvastava teabe (PII) kaitse.	Organisatsioon tuvastab ja täidab privaatsuse kaitse nõudeid vastavalt kehtivatele seadustele ja määrustele ning lepingunõuetele	JAH
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
5.36	Infoturbe poliitikate, reeglite ja standardite järgimine	Korrapäraselt vaadatakse üle organisatsiooni infoturbepoliitika, kõrgeimate turvapõhiste poliitikate, reeglite ja standardite järgimine.	JAH
5.37	Dokumenteeritud tööprotseduurid	Infotöötlusseadmete töökord dokumenteeritakse ja tehakse seda vajavale personalile kättesaadavaks.	JAH
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
6.2	Töötingimused	Töölepingutes on määratletud personali ja organisatsiooni kohustused infoturbe valdkonnas.	JAH
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

Kood	Kontrollid	Meede	Kohaldub JAH/EI
6.4	Distsiplinaarprotsess	Infoturbepoliitika rikkumise toime pannud töötajate ja teiste huvitatud isikute suhtes algatatakse distsiplinaarmenetlus	JAH
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
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
6.7	Kaugtöö	Kui töötajad töötavad eemalt, tuleb rakendada turvameetmeid, et kaitsta teavet, millele juurdepääs, mida töödeldakse või säilitatakse väljaspool organisatsiooni ruume.	JAH
6.8	Infoturbe sündmuste aruandlus	Organisatsioon peab tagama töötajatele võimaluse õigeaegselt teavitada täheldatud või kahtlustatavatest infoturbesündmustest sobivate kanalite kaudu	JAH
7.	Füüsilised kontrollid		
7.1	Füüsilise turvalisuse perimeetrid	Füüsilised piirid on määratletud ja neid kasutatakse turvaalade ja ettevõtte varade kaitsmiseks	JAH
7.2	Sissepääs turvaalale on kontrollitud	Turvaalade jaoks tuleks määratleda sisenemispunktid ja juurdepääsureeglid	JAH
7.3	Kontorite, ruumide ja rajatiste turvamine	Kontorite, ruumide ja rajatiste füüsiline perimeeter on kindlustatud.	JAH
7.4	Füüsilise turvalisuse jälgimine	Ruumides tuleb pidevalt jälgida selleks volitatud isikuid	JAH
7.5	Kaitsmine füüsiliste ja keskkonnaohtude eest	Kavandage ja rakendage meetmeid füüsiliste ja keskkonnaohtude korral (looduskatastroofid, ebasobiv keskkond, füüsilised ohud)	JAH
7.6	Juurdepääs turvalistele aladele	Turvaaladele juurdepääsureeglid on määratletud ja rakendatud	JAH
7.7	Selge laud ja selge ekraan	Läbipaistva laua, printimise ja eemaldatava kandja ning selge ekraani reeglid; määratletakse ja jõustatakse teabetöötlusseadmete reeglid.	JAH
7.8	Seadmete paigutus ja kaitse	Seadmed peavad olema kindlas kohas ja kaitstud	JAH
7.9	Varade turvalisus väljaspool äriruume	Väljaspool objekti asuv vara tuleb kaitsta.	JAH
7.10	Andmekandja	Säilituskandjaid hallatakse kogu nende soetamise, kasutamise, transportimise ja kõrvaldamise elutsükli jooksul vastavalt organisatsiooni klassifitseerimisskeemile ja käitlemisnõuetele.	JAH

Kood	Kontrollid	Meede	Kohaldub JAH/EI
7.11	Kommunaalteenuste toetamine	Infotöötlusrajatised peavad olema kaitstud elektrikatkestuste ja muude tugiteenuste riketest põhjustatud häirete eest	JAH
7.12	Kaabli turvalisus	Toite-, andme- või tugiteabeteenuseid kandvad kaablid peavad olema pealtkuulamise, häirete või kahjustuste eest kaitstud	JAH
7.13	Seadmete hooldus	Seadmeid tuleb korralikult hooldada, et tagada teabe kättesaadavus, terviklikkus ja konfidentsiaalsus	JAH
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
8.	Tehnoloogilised kontrollid		
8.1	Kasutaja lõpp-punkti seadmed	Kasutajaseadmete kaudu salvestatud, töödeldud või juurdepääsetav teave peab olema kaitstud.	JAH
8.2	Privilegeeritud juurdepääsuõigused	Privilegeeritud juurdepääsuõiguste eraldamine ja kasutamine on piiratud ja hallatud	JAH
8.3	Andmetele juurdepääsu piirang	Juurdepääs andmetele ja nendega seotud varadele tuleb piirata vastavalt kehtestatud subjektipõhisele juurdepääsukontrolli poliitikale	JAH
8.4	Juurdepääs lähtekoodile	Lugemis- ja kirjutamisjuurdepääsu lähtekoodile, arendustööriistadele ja tarkvarateekidele tuleb asjakohaselt hallata.	JAH
8.5	Turvaline autentimine	Turvalist autentimist rakendatakse teabe juurdepääsupiirangute ja juurdepääsu kontrollimise poliitikate alusel	JAH
8.6	Võimsuse juhtimine	Ressursikasutust jälgitakse ja kohandatakse lähtuvalt praegusest ja eeldatavast võimsusvajadusest.	JAH
8.7	Kaitse pahavara eest	Pahavaravastane kaitse peab olema rakendatud ja seda peab toetama asjakohane kasutajateadlikkus.	JAH
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
8.9	Konfiguratsiooni juhtimine	Luuakse, dokumenteeritakse, rakendatakse, jälgitakse ja vaadatakse üle riistvara, tarkvara, teenuste ja võrkude konfiguratsioonid, sealhulgas turbekonfiguratsioonid.	JAH
8.10	Teabe kustutamine	Infosüsteemides, seadmetes või muudel andmekandjatel salvestatud teave kustutatakse, kui seda enam ei vajata	JAH

Kood	Kontrollid	Meede	Kohaldub JAH/EI
8.11	Andmete maskeerimine	Andmete maskeerimist kasutatakse vastavalt organisatsiooni subjektipõhisele juurdepääsukontrolli poliitikale ja muudele seotud teemapõhistele põhimõtetele ja ärinõuetele, võttes arvesse kehtivaid seadusi.	JAH
8.12	Andmelekke vältimine	Andmelekke vältimise meetmeid rakendatakse süsteemide, võrkude ja muude seadmete puhul, mis töötlevad, salvestavad või edastavad tundlikku teavet	JAH
8.13	Teabe varundamine	Teabe, tarkvara ja süsteemide varukoopiaid tuleb hooldada ja regulaarselt testida vastavalt kokkulepitud teemapõhisele varunduspoliitikale	JAH
8.14	Infotöötlusseadmete koondamine	Teabetöötlusrajatised on rakendatud piisava koondamisega, et vastata kättesaadavusnõuetele.	JAH
8.15	Logimine	Luuakse, hooldatakse, kaitstakse ja analüüsitakse logisid, mis salvestavad tegevusi, erandeid, vigu ja muid asjakohaseid sündmusi.	JAH
8.16	Seiretegevused	Võrke, süsteeme ja rakendusi jälgitakse ebatavalise käitumise suhtes ning rakendatakse asjakohaseid meetmeid võimalike infoturbeintsidentide hindamiseks	JAH
8.17	Kella sünkroonimine	Organisatsioonis kasutatavate infotöötlussüsteemide kellad peavad olema sünkroniseeritud ja kontrollitud.	JAH
8.18	Privilegeeritud utiliitprogrammide kasutamine	Süsteemi ja rakenduste juhtelemente segavate utiliitprogrammide kasutamine peab olema piiratud ja rangelt kontrollitud	JAH
8.19	Tarkvara installeerimine operatsioonisüsteemidesse	Rakendatakse protseduure ja meetmeid tarkvara installimise turvaliseks haldamiseks operatsioonisüsteemidesse	JAH
8.20	Võrkude turvalisus	Võrgud ja võrguseadmed peavad olema kaitstud, hallatud ja kontrollitud, et kaitsta süsteemides ja rakendustes sisalduvat teavet.	JAH
8.21	Võrguteenuste turvalisus	Tuvastatakse, rakendatakse ja jälgitakse võrguteenuste turvamehhanisme, teenusetasemeid ja teenusenõudeid	JAH
8.22	Võrkude eraldamine	Infoteenuste, kasutajate ja infosüsteemide rühmad peavad olema organisatsiooni võrkudes eraldatud.	JAH
8.23	Veebi filtreerimine	Juurdepääsu välistele veebisaitidele hallatakse pahatahtliku sisuga kokkupuute minimeerimiseks.	JAH
8.24	Krüptograafia kasutamine	Määratletakse ja rakendatakse krüptograafia tõhusa kasutamise reeglid, sealhulgas krüptograafilise võtme haldamise reeglid	JAH
8.25	Turvaline arenduse elutsükkel	Kehtestatakse ja rakendatakse reeglid tarkvara ja süsteemide ohutuks arendamiseks.	JAH

Kood	Kontrollid	Meede	Kohaldub JAH/EI
8.26	Rakenduse turvanõuded	Infoturbe nõuded tuvastatakse, täpsustatakse ja kinnitatakse rakenduse arendamise või hanke käigus.	JAH
8.27	Turvaline süsteemi arhitektuur ja põhimõtted	Turvaliste süsteemide kujundamise põhimõtted kehtestatakse, dokumenteeritakse, hooldatakse ja rakendatakse kõigis infosüsteemide arendustegevustes.	JAH
8.28	Turvaline kodeerimine	Tarkvaraarenduses rakendatakse turvalise kodeerimise põhimõtteid	JAH
8.29	Turvatestimine arenduses ja vastuvõtmisel	Turvatestimise protsessid määratletakse ja rakendatakse kogu arenduse elutsükli jooksul	JAH
8.30	Väljastpoolt tellitud arendus	Organisatsioon juhib, jälgib ja vaatab üle sisseostetava süsteemiarendusega seotud tegevusi.	EI
8.31	Arendus- ja testkeskkondade eraldamine	Arendus-, testi- ja kasutuskeskkonnad peavad olema eraldatud ja kaitstud.	JAH
8.32	Muutuste juhtimine	Infotöötlusvahendite ja infosüsteemide muudatustele kohaldatakse muudatuste haldamise korda.	JAH
8.33	Testi andmed	Testiandmed peavad olema õigesti valitud, kaitstud ja hallatud	JAH
8.34	Infosüsteemide kaitse auditi testimise ajal	Audititestid ja muud operatsioonisüsteemide hindamist hõlmavad tegevused planeeritakse ja lepitakse testija ja ettevõtte vahel kokku	JAH