

ISO/IEC 27001:2022 + Amd 1:2024 Infoturbe halduse süsteemid (ISMS)

Infoturve, ISMS, kogu maailmas sertifitseeritav

181 nõuet. Selle standardi järgi on võimalik sertifitseerida akrediteeritud sertifitseerimisasutuses. Versioon 07/2026.

ISO/IEC 27001 sätestab nõuded infoturbe halduse süsteemile: riskipõhine, dokumenteeritud ja tõendatavalt tulemuslik. Hindamine selle vastu on akrediteeritud sertifitseerimisaudit kahes etapis (dokumentide ülevaatus, seejärel tulemuslikkuse hindamine kohapeal), millele järgnevad iga-aastased järelevalveaudidid ja resertifitseerimine kolme aasta pärast.

Ettevõtte	Kuupäev	Täitja
-----------	---------	--------

4 Organisatsiooni kontekst

8

4.1-1 Välised ja sisemised teemad, mis mõjutavad organisatsiooni võimet saavutada ISMS kavandatud tulemusi, on kindlaks määratud ja hoitakse ajakohasena.

Mille järgi seda näeb: Tõendiks on kontekstianalüüs kas eraldi dokumendina või ISMS käsiraamatu osana: turukeskkond, kliendi ja lepingute olukord, õigusraamistik (GDPR, NIS2), kasutatav tehnoloogiavõrk, töötajate arv, sõltuvus pilveteenuse pakkujatest. Väikeses ettevõttes piisab ühe lehekülje tabelist koos kuupäeva ja ülevaatus sagedusega, kui juhtkonnapoolne ülevaatus näitab, et seda ka tegelikult ajakohastatakse.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.1-2 Organisatsioon on kindlaks määranud, kas kliimamuutus on tema jaoks oluline teema. Tulemus on põhjendatud sõltumata sellest, kas vastus on jah või ei.

Mille järgi seda näeb: See nõue tuli Amd 1:2024 muudatusega ja audiitorid küsivad seda eraldi. Kontekstianalüüsis on mõistlik hoida omaette rida: kuumaperioodid, mis mõjutavad serveriruumi ja käideldavust, äärmuslik ilm, mis mõjutab pilveteenuse pakkuja andmekeskusi, elektrivõrgu stabiilsus. Põhjendatud tulemus, et teema ei ole oluline, on vastuvõetav, puuduv kanne aga mitte.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.2-1 Huvipooled, kes on ISMS seisukohalt asjakohased, on kindlaks määratud.

Mille järgi seda näeb: Huvipoolte loend, mis katab kliendid, töötajad, volitatud töötajad ja alltöötajad, järelevalveasutused, kindlustusandjad, sertifitseerimisasutuse ja osanikud. Väikeses ettevõttes piisab tabelist, kus on huvipool, ootus ja ootuse allikas.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.2-2 Nende huvipoolte asjakohased nõuded on kindlaks määratud, sealhulgas kliimamuutusega seotud nõuded.

Mille järgi seda näeb: Iga huvipoolte juures on nimetatud konkreetne allikas: lepingupunkt, andmetöötlusleping, kliendi küsimustik, õiguslik kohustus. Amd 1:2024 lisab märkuse, et huvipooltel võib olla kliimamuutusega seotud nõudeid. Tegemist ei ole eraldi kohustusliku nõudega, kuid audiitorid tõstatavad selle tavapäraselt, näiteks suurtööstuse tarnijaauditi kestlikkuse küsimustena. Piisab ühest reast huvipoolte tabelis koos tulemusega, sealhulgas tulemusega, et selliseid nõudeid ei ole.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.2-3 On otsustatud ja jälgitav, milliseid neist nõuetest käsitletakse ISMS kaudu.

Mille järgi seda näeb: Huvipoolte tabelisse lisatud veerg viitab reeglile, mis nõuet käsitleb (poliitika, ohjemeede, lepingu lisa). Nii on näha, et nõudeid ei ole üksnes kogutud, vaid ka tegelikult läbi töötatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.3-1 ISMS käsitusala on kindlaks määratud ja arvestab punkti 4.1 teemasid, punkti 4.2 nõudeid ning liideseid ja sõltuvusi kolmandate poolte tegevustega.

Mille järgi seda näeb: Käsitusala nimetab asukohad, organisatsiooniüksused, tooted, süsteemid ja võrgupiirid. Sisseostetud osad (majutus, makseteenuse pakkujad, tugi) on kirjeldatud liidestena koos selge vastutuspiiriga. Kunstlikult kitsendatud käsitusala, mis jätab põhiprotsessid välja, lükkavad sertifitseerimisasutused tagasi.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.3-2 Käsitusala on kättesaadav dokumenteeritud teabena ja esitab ISMS piirid ühemõtteliselt.[Dokument](#)

Mille järgi seda näeb: Kinnitatud käsitusala dokument koos versiooni, kuupäeva ja tippjuhtkonna heakskiiduga. Selle täpne sõnastus jõuab hiljem sertifikaadile, seega on sõnastus täpne ja avalikult tsiteeritav.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

4.4-1 ISMS koos vajalike protsesside ja nende koostoimega on kehtestatud, rakendatud, ajakohasena hoitud ja pidevalt parendatud.

Mille järgi seda näeb: Protsessikaart või protsesside loend, mis seob riskihalduse, juhtumite käsitlemise, muudatuste halduse, auditeerimise ja juhtkonnapoolse ülevaatused koos omanike ja sagedusega. Elav tõend kaalub rohkem kui skeem: piletid, protokollid, kalendrikanded.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5 Eestvedamine

8

5.1-1 Tippjuhtkond võtab vastutuse ISMS tulemuslikkuse eest ning tagab poliitika ja eesmärkide kehtestamise kooskõlas strateegilise suunaga.

Mille järgi seda näeb: Tõendiks on poliitika, käsitusala ja rakendatavuse avalduse allkirjastatud kinnitused, juhtkonnapoolse ülevaatused, protokollid ja dokumenteeritud eelarveotsused. Väga väikeses ettevõttes on tippjuhtkond sageli sama isik kui ISMS omanik, mis on vastuvõetav, kui see on rollide kirjelduses avalikult välja öeldud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.1-2 ISMS nõuded on lõimitud äriprotsessidesse ja tulemusliku infoturbe tähtsust kommunikeeritakse.

Mille järgi seda näeb: Kõige paremini näitab seda olukord, kus turve ei ole eraldi kaustas: turbekriteerium valmis töö kriteeriumides, turbekontroll müügi või hanke protsessis, korduv turbeteema meeskonnakoosoleku protokollis.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.1-3 Juhtkond annab vajalikud ressursid, toetab inimesi, kes panustavad ISMS tulemuslikkusesse, ja edendab pidevat parendamist.

Mille järgi seda näeb: Kinnitatud turbeelarve, koolituseks eraldatud aeg, väliste audiitorite või läbistustestijate kaasamine. Parendus- või tegevusregister kannetega mitme kvartali ulatuses näitab järjepidevust ühekordse pingutuse asemel.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.2-1 Infoturbepoliitika on kehtestatud, see sobib organisatsiooni eesmärgiga ja annab raamistiku infoturbe eesmärkidele.[Dokument](#)

Mille järgi seda näeb: Lühike kinnitatud poliitikadokument, kaks kuni kolm lehekülge on piisav. See nimetab kaitse-eesmärgid, käsitusala, vastutused ja riskipõhise lähenemise põhimõtte. Üldine mallitekst, millel puudub seos tegeliku tegevusega, torkab auditis silma.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.2-2 Poliitika sisaldab kohustust täita kohalduvaid nõudeid ja kohustust ISMS pidevaks parendamiseks.[Dokument](#)

Mille järgi seda näeb: Mõlemad kohustused on poliitikas selgesõnaliste lausetena olemas ja need loetakse 1. etapi auditis sõna-sõnalt läbi. Lisaks viitab poliitika aluseks olevatele protsessidele (õigusaktide register, parendusregister).

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.2-3 Poliitikat kommu­ni­keeritakse organisatsiooni sees ja see on huvipooltele kättesaadav vastavalt vajadusele.[Dokument](#)

Mille järgi seda näeb: Tõendiks on sisevõrgu või viki kanne koos lugemiskohustusega, sisseelamise kontroll-leht kinnitusega või avaldatud kokkuvõtte veebilehel. Levitusloend koos lugemiskinnitustega on kõige lihtsam kindel tõend.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.3-1 Turbega seotud rollide vastutused ja volitused on määratud ja organisatsiooni sees kommu­ni­keeritud.

Mille järgi seda näeb: Rollimaatriks (RACI), mis katab ISMS omaniku, riskiomanikud, varaomanikud, juhtumite koordinaatori ja andmekaitse kontaktisiku. Ühe­ni­me­se- või väga väikestes meeskondades on iga roll määratud nimeliselt ja tekkiv rollide kuhjumine on avalikult dokumenteeritud, mitte varjatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.3-2 Volitus tagada ISMS vastavus standardile ja anda tippjuhtkonnale aru ISMS toimivusest on määratud ühele rollile.

Mille järgi seda näeb: ISMS omaniku määramiskiri või rollikirjeldus koos selgesõnalise aruandlusliiniga juhtkonnale. Aruandlusliin on tegelikult tõendatud juhtkonnapoolse ülevaatus protokollidega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6 Planeerimine

21

6.1.1-1 Punkti 4.1 teemadest ja punkti 4.2 nõuetest lähtudes on kindlaks määratud riskid ja võimalused, mida käsitletakse, et ISMS saavutaks kavandatud tulemused ja soovimatud mõjud oleksid välditud.

Mille järgi seda näeb: Register, mis seob konteksti teemad riskide ja võimalustega, eraldi või riskiregistri sees. Oluline on jälgitavus: iga kontekstianalüüsi teema viib nähtavalt hindamiseni või põhjendatud otsuseni seda mitte arvestada.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.1-2 Nende riskide ja võimaluste käsitlemise tegevused on kavandatud, lõimitud ISMS protsessidesse ja nende tulemuslikkust hinnatakse.

Mille järgi seda näeb: Tegevuskava koos vastutaja, tähtaja ja tulemuslikkuse kriteeriumiga. Tulemuslikkuse hindamine on omaette veerus, muidu puudub auditis tõend, et tegevus ei olnud üksnes ellu viidud, vaid ka üle kontrollitud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.2-1 Infoturbe riskihindamise protsess on määratletud ja rakendatud; see sisaldab riski aktsepteerimise kriteeriume ja riskihindamiste tegemise kriteeriume.[Dokument](#)

Mille järgi seda näeb: Riskihalduse poliitika koos tõenäosuse ja mõju skaaladega, määratletud riskimaatriks ja selge aktsepteerimislävend. Lävend on arv või tsoon, mitte sõnastus stiilis meie äranägemisel.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.2-2 Protsess tagab, et korduvad riskihindamised annavad järjepidevaid, kehtivaid ja võrreldavaid tulemusi.

Mille järgi seda näeb: Tõendiks on kindel metoodika määratletud skaaladega ja kahe hindamisversiooni võrdlus: samad riskid, sama hindamisloogika, selgitatavad erinevused. Kuupäevastatud eelmise aasta riskiregistri versioon on siin kõige tugevam tõend.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.2-3 Infoturbe riskid on tuvastatud, et avastada konfidentsiaalsuse, tervikluse ja käideldavuse kadu käsitusallas, ning igale riskile on määratud riskiomanik.

Mille järgi seda näeb: Riskiregister, mis viitab varadele või protsessidele, kolmele kaitse-eesmärgile ja nimelisele riskiomanikule. Riskiomanikul on volitus riski aktsepteerida; väikeses ettevõttes on selleks tavaliselt juhatuse liige.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.2-4 Tuvastatud riske analüüsitakse: võimalikud tagajärjed, realistlik tõenäosus ja neist tulenev riskitase on kindlaks määratud.

Mille järgi seda näeb: Veerud mõju, tõenäosuse ja tulemuseks oleva riskitaseme jaoks, igaüks koos lühikese põhjendusega. Üks lause põhjendust riski kohta hoiab ära kõige sagedasema auditileiu, milleks on tuletuseta arvud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.2-5 Riske võrreldakse aktsepteerimiskriteeriumidega ja seatakse käsitlemiseks tähtsuse järjekorda.

Mille järgi seda näeb: Riskiregistrist on näha, millised riskid jäävad aktsepteerimislävendist kõrgemale ja millises järjekorras neid käsitletakse. Piisab sorteeritud vaatest või prioriteedi veerust.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.2-6 Riskihindamise protsess on kättesaadav dokumenteeritud teabena.[Dokument](#)

Mille järgi seda näeb: Metoodika ise on kohustuslik dokument, mitte üksnes selle väljund. Kinnitatud poliitika koos versiooni ja kinnitamise kuupäevaga, viidatud ISMS dokumendiregistris.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-1 Igale aktsepteerimislävendist kõrgemale jäävale riskile on valitud sobiv käsitlemisviis (vähendada, vältida, üle anda või aktsepteerida).

Mille järgi seda näeb: Käsitlemisviisi veerg riskiregistris. Kui risk aktsepteeritakse, registreeritakse põhjendus ja riskiomaniku ametlik heakskiit; kui risk antakse üle, nimetatakse lepingu või kindlustuspoliisi.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-2 Kõik ohjemeetmed, mis on valitud riskikäsitlemisviiside rakendamiseks vajalikud, on kindlaks määratud.

Mille järgi seda näeb: Ohjemeetmed on sõnastatud konkreetsete ja kontrollitavate, koos vastutaja ja tähtajaga. Viide juba käimasolevale tehnilisele tööle (MFA kasutuselevõtt, varukoopia test) sobib, kui see osutab piletile või konfiguratsiooni artefaktile.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-3 Kindlaks määratud ohjemeetmeid võrreldakse lisa A ohjemeetmetega, et tõendada, et ükski vajalik ohjemeede ei ole kahe silma vahele jäänud.

Mille järgi seda näeb: Võrdlus on eraldi jälgitav samm, mitte kõrvalsaadus. Tõendiks on riskiregistri kaardistusveerg, mis viitab lisa A numbritele, ja kuupäevastatud protokoll võrdluse kohta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-4

Rakendatavuse avaldus (SoA) on olemas. See hindab kõiki 93 lisa A ohjemeedet ükshaaval, esitab iga ohjemeetme rakendatavuse koos põhjendusega, rakendamise seisu ja iga väljajätmise põhjenduse.[Dokument](#)

Mille järgi seda näeb: SoA on keskne kohustuslik dokument ja kogu auditi kaart. See on täielik: ohjemeetmed, mis ei ole rakendatavad, on samuti esitatud koos põhjendusega, mitte kunagi tühja reana. Soovituslikud veerud: ohjemeetme number, nimetus, rakendatav jah või ei, põhjendus, rakendamise seis, viide poliitikale või tõendile, seos riskiga. Versioon ja juhtkonna heakskiit on kohustuslikud, sest SoA võrreldakse tegelikkusega igal järelevalveauditiil.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-5

Riskikäsitlemise plaan on koostatud ja see koondab ohjemeetmed, vastutused, tähtajad ja vajalikud ressursid.[Dokument](#)

Mille järgi seda näeb: Selleks sobib riskitabeli eraldi leht või projektitahvel. Loeb see, et tähtajad on realistlikud ja et möödalastud tähtajad on nähtavalt ümber planeeritud, sest just seda audiitor kontrollib.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-6

Riskikäsitlemise plaani on riskiomanikud heaks kiitnud ja allesjäävad jääkriskid ametlikult aktsepteerinud.[Dokument](#)

Mille järgi seda näeb: Allkiri, elektrooniline heakskiit või kuupäevastatud otsus protokollis. Piisab ühest reast juhtkonnapoolse ülevaatuse protokollis koos viitega registri versioonile, kui versioon on ühemõtteline.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.1.3-7

Riskikäsitlemise protsess on kättesaadav dokumenteeritud teabena.[Dokument](#)

Mille järgi seda näeb: Tavaliselt kaetud sama poliitikadokumendiga kui riskihindamine. Kirjeldatud on kulg hindamisest käsitlemisviisi valiku kaudu jääkriski aktsepteerimiseni.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.2-1

Infoturbe eesmärgid on kehtestatud asjakohastele funktsioonidele ja tasanditele, on kooskõlas poliitikaga ja on mõõdetavad, kus see on teostatav.

Mille järgi seda näeb: Eesmärkide leht kolme kuni kuue eesmärgiga, igaühel mõõdik, lähtetase, sihtväärtus ja tähtaeg. Näiteks: MFA-ga süsteemide osakaal tõstetud 80 protsendilt 100 protsendile kvartali lõpuks. Eesmärgid ilma arvuta loetakse mittemõõdetavaks.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.2-2

Eesmärgid arvestavad kohalduvaid infoturbe nõudeid ning riskihindamise ja riskikäsitlemise tulemusi.

Mille järgi seda näeb: Eesmärkide lehele lisatud päritolu veerg näitab, millisest riskist, kliendinõudest või õiguslikust kohustusest eesmärk pärineb. Nii välditakse eesmarke, mis mõjuvad meelevaldselt.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.2-3

Eesmarke seiratakse, kommunikeeritakse ja ajakohastatakse vastavalt vajadusele.

Mille järgi seda näeb: Kvartaalne edenemise jälgimine eesmärkide lehel ja teavitus meeskonnale, näiteks lühike märged vikis või päevakorrapunkt meeskonnakoosolekul. Varasemad versioonid näitavad, et ajakohastamine toimub.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

6.2-4 Infoturbe eesmärgid on kättesaadavad dokumenteeritud teabena.[Dokument](#)

Mille järgi seda näeb: Piisab kinnitatud eesmärkide dokumendist koos kuupäevaga. See võib olla juhtkonnapoolse ülevaatuse osa, kuid on seal omaette leitava jaotisena olemas.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)**6.2-5 Iga eesmärgi kohta on kavandatud, mida tehakse, milliseid ressursse vajatakse, kes vastutab, millal see valmib ja kuidas tulemusi hinnatakse.**

Mille järgi seda näeb: Need viis punkti on eraldi kontrollitavad ja neid küsitakse auditis eraldi. Eesmärkide lehel viie veeruna seatuna on vastavus ühe pilguga näha.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)**6.3-1 Kui organisatsioon määrab kindlaks, et ISMS vajab muudatusi, viiakse need muudatused ellu kavandatud viisil.**

Mille järgi seda näeb: Tõendiks on muudatustaotlused, protokollid või piletid, millest nähtub ajend, mõju hindamine, heakskiit ja elluviimine. Tüüpilised ajendid väikeses ettevõttes: pilveteenuse pakkuja vahetus, uued asukohad, esimene töötaja.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)**7 Tugi**

15

7.1-1 ISMS kehtestamiseks, rakendamiseks, ajakohasena hoidmiseks ja pidevaks parendamiseks vajalikud ressursid on kindlaks määratud ja antud.

Mille järgi seda näeb: Turbeelarve rida, tööriistade litsentsid (paroolihaldur, MDM, logiplatvorm), ISMS ülalpidamiseks planeeritud inimpäevad ja välised auditeerimisteenused. Arve või eelarve kinnitus tõendab seda kiiremini kui igasugune tekst.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)**7.2-1 Nende inimeste vajalik pädevus, kelle töö mõjutab infoturbe toimivust, on kindlaks määratud.**

Mille järgi seda näeb: Pädevusmaatriks või rolliprofiilid, mis loetlevad rolli kohta vajalikud teadmised, näiteks turvaline arendus arendajatele, juhtumite käsitlemine koordinaatorile. Väga väikestes meeskondades piisab ühest reast inimese kohta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)**7.2-2 Pädevus on tagatud sobiva hariduse, koolituse või kogemuse alusel.**

Mille järgi seda näeb: Tunnistused, koolituse kinnitused, elulookirjeldused või dokumenteeritud praktiline kogemus. Iseseisev õppimine on vastuvõetav, kui see on tõendatud, näiteks veebikursuste läbimise kirjetega või läbitud sisemiste teadmiskontrollidega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)**7.2-3 Kui pädevuses on lünki, on nende sulgemiseks tegevused ellu viidud ja nende tegevuste tulemuslikkust on hinnatud.**

Mille järgi seda näeb: Koolituskava koos plaani ja tegeliku täitmise võrdlusega ning tulemuslikkuse kontrolliga, näiteks testi tulemus, andmepüügi simulatsiooni klikimäär või töökohal tehtud vaatlus. Tulemuslikkuse kontroll ununeb tihti ja on klassikaline väike leid.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

[Tõend / põhjendus](#)

7.2-4 Pädevuse tõendina on kättesaadav asjakohane dokumenteeritud teave.[Dokument](#)

Mille järgi seda näeb: Pädevuse või koolituse kaust iga inimese kohta koos tõendite ja kuupäevadega. Väikeses ettevõttes piisab kataloogist salvestatud PDF-kirjetega ja ülevaetatabelist.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.3-1 Käsitusallas töötavad inimesed on infoturbepoliitikaga kursis.

Mille järgi seda näeb: Kinnitus sisseelamisel ja pärast iga muudatust poliitikas, koos kuupäeva ja versiooniga. Piisab viki lugemiskinnituse funktsioonist või allkirjastatud loendist.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.3-2 Inimesed teavad oma panust ISMS tulemuslikkusesse ja parema infoturbe toimivuse kasu.

Mille järgi seda näeb: Koolitusmaterjal ja osalejate loendid, milles on nähtav seos inimese enda tööga. Audiitorid küsitlevad töötajaid otse, seega toimub koolitus konkreetsete igapäevaste näidete varal, mitte standardi abstraktsete tsitaatide varal.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.3-3 Inimesed teavad ISMS nõuete täitmata jätmise tagajärgi.

Mille järgi seda näeb: Tagajärjed on kirjas koolitusslaididel ja tööjuhendites ning seotud protsessiga punkti A.6.4 all. Ka töötajateta ettevõtte katab selle lepingupartnerite ja vabakutseliste puhul lepingute kaudu.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.4-1 ISMS jaoks oluline sise- ja väliskommunikatsioon on kindlaks määratud: mida kommunikeeritakse, millal, kellega ja milliste vahenditega.

Mille järgi seda näeb: Kommunikatsioonimaatriks ridadega nagu turvajuhtum klientidele, teavitus järelevalveasutusele 72 tunni jooksul, igakuine seisuaruanne juhtkonnale. See on kriisikommunikatsiooni alus ja vaadatakse üle pärast iga juhtumit.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.5.1-1 ISMS hõlmab standardi nõutavat dokumenteeritud teavet ning dokumenteeritud teavet, mille organisatsioon on ISMS tulemuslikkuse jaoks vajalikuks pidanud.[Dokument](#)

Mille järgi seda näeb: Dokumendiregister, mis loetleb iga ISMS dokumendi koos otstarbe, omaniku, versiooni ja hoiukohaga. See näitab, et kohustuslikud dokumendid on täielikud, ja on audiitorile kiireim sisenemispunkt.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.5.2-1 Dokumentide loomisel ja ajakohastamisel on tagatud sobiv tähistus, vorming ja andmekandja ning dokumendid vaadatakse üle ja kiidetakse sobivuse osas heaks.

Mille järgi seda näeb: Ühtne dokumendipäis pealkirja, versiooni, kuupäeva, autori ja kinnitajaga. Git-põhises keskkonnas täidavad heakskiiduga muudatustootluste ülevaatused ülevaatus ja kinnitamise nõuet, kui ajalugu on muutumatu.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.5.3-1 Vajalikus kohas ja vajalikul ajal on dokumenteeritud teave kättesaadav ja kasutuskõlblik.

Mille järgi seda näeb: Keske hoiukoht, mille juurde pääsevad kõik õigustatud inimesed, koos otsingufunktsiooniga. Kontrollitav pistelise valikuga: iga tööjuhend on leitav vähem kui minutiga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.5.3-2 Dokumenteeritud teave on piisavalt kaitstud, eelkõige konfidentsiaalsuse kao, väärkasutuse ja tervikluse kao vastu.

Mille järgi seda näeb: Rollipõhised pääsuõigused ISMS dokumentidele, versioonihaldus koos ajalooga, kirjutuskaitse kinnitatud versioonidele ja dokumendihoidla varukoopia. Varukoopia tõend ununeb kõige sagedamini.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.5.3-3 Dokumenteeritud teabe levitamine, pääs, väljaotsimine, hoiustamine, muudatuste ohjamine ning säilitamine ja hävitamine on reguleeritud.

Mille järgi seda näeb: Lühike dokumendiohje reegel koos säilitustähtaegade ja kustutamisreeglitega. See on kooskõlla viidud õiguslike kohustustega (äriõigus, maksuõigus, GDPR) ja on aluseks punktidele A.5.33 ja A.8.10.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

7.5.3-4 Välise päritoluga dokumenteeritud teave, mis on ISMS planeerimiseks ja käitamiseks vajalik, on tuvastatud ja ohjatud.

Mille järgi seda näeb: Väliste dokumentide loend koos versiooni ja allikaga: standardid, õigusaktid, tootjate turvakarastuse juhendid, pilveteenuse turbedokumentatsioon, andmetöötluslepingud. Ilma versiooniviiteta ei ole ohjet võimalik tõendada.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8 Toimimine

8

8.1-1 Infoturbe nõuete täitmiseks ja peatüki 6 tegevuste elluviimiseks vajalikud protsessid on kavandatud, rakendatud ja ohjatud ning nendele protsessidele on kehtestatud kriteeriumid.

Mille järgi seda näeb: Käitamiskäsiraamat või tegevusjuhendid selgete kriteeriumidega, näiteks kriitiliste paikade paigaldamise maksimaalne aeg, väljalaskekriteeriumid juurutustele, häirelävendid. Arvudeta kriteeriumid ei ole auditis midagi väärt.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.1-2 Kindluse saamiseks, et protsessid on kavandatud viisil läbi viidud, on dokumenteeritud teave kättesaadav vajalikus ulatuses.[Dokument](#)

Mille järgi seda näeb: Käitamise kirjed tõendina: piletite ajalugu, CI konveieri käivitused, paikamise aruanded, varukoopia logid, pääsuõiguste ülevaatused. Need kirjed on 2. etapi auditis tegelik tulemuslikkuse tõend.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.1-3 Kavandatud muudatusi ohjatakse ja tahtmatute muudatuste tagajärjed vaadatakse üle; vajaduse korral leevendatakse ebasoodsaid mõjusid.

Mille järgi seda näeb: Muudatuste protsess koos heakskiidu ja tagasipööramise teega, seotud punktiga A.8.32. Tahtmatute muudatuste puhul (vale seadistus, kogemata antud kõrgendatud õigused) dokumenteeritakse juhtum ja tõendatakse parandus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.1-4 Väljastpoolt hangitud protsessid, tooted ja teenused, mis on ISMS seisukohalt olulised, on kindlaks määratud ja ohjatud.

Mille järgi seda näeb: Tarnijate loend koos kriitilisuse, lepinguviite ja tõendite seisuga (tarnija ISO 27001 sertifikaat, SOC 2 aruanne, andmetöötlusleping). Väikese ettevõtte jaoks on see suurim hoob, sest suurem osa IT-st käib niikuinii väljaspool maja.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.2-1 Riskihindamisi tehakse kavandatud sagedusega ja alati, kui toimuvad olulised muudatused või juhtumid, arvestades kehtestatud kriteeriume.

Mille järgi seda näeb: Rütm (tavaliselt kord aastas) ja määratletud ajendid plaaniväliseks hindamiseks. Tõendiks on riskiregistri kuupäevastatud versioonid ja kanded kalendris või piletisüsteemis.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

8.2-2 Riskihindamiste tulemusi säilitatakse dokumenteeritud teabena.

Dokument

Mille järgi seda näeb: Riskiregistri varasemad versioonid koos kuupäevadega, mitte üksnes praegune seis. Faili ülekirjutamine muudab arengu tõendamatuks; failisüsteemi või Giti versioonihaldus lahendab selle.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

8.3-1 Riskikäsitlemise plaan on ellu viidud.

Mille järgi seda näeb: Plaani ja tegelikkuse võrdlus: lõpetatud tegevused koos elluviimise kuupäeva ja konkreetse artefaktiga (konfiguratsioon, poliitika, leping). Lõpetamata tegevustel on dokumenteeritud põhjendus ja uus sihtkuupäev.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

8.3-2 Riskikäsitlemise tulemusi säilitatakse dokumenteeritud teabena.

Dokument

Mille järgi seda näeb: Seisuaruanded või suletud tegevused koos viitega tõendile. Registrist üksi piisab, kui igal real on lõpetamise kuupäev ja link tõendile.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

9 Toimivuse hindamine

21

9.1-1 Kindlaks on määratud, mida seiratakse ja mõõdetakse, sealhulgas infoturbe protsessid ja ohjemeetmed.

Mille järgi seda näeb: Mõõdikute leht hallatava arvu kindlate mõõdikutega: paikamise järjekord, MFA katvus, juhtumite lahendamise aeg, viimase taastamise testi tulemus, avatud leiud. Mõned tegelikult kogutavad mõõdikud kaaluvad üles pika soovinimekirja.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

9.1-2 Seire, mõõtmise, analüüsi ja hindamise meetodid on määratletud ja annavad kehtivaid tulemusi.

Millie järgi seda näeb: Iga mõõdiku juures on dokumenteeritud andmeallikas ja arvutuskäik, näiteks väljavõte haavatavuste skannerist või identiteedipakkaja aruandest. Allika jälgitavus on kehtivuse tuum.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

9.1-3 Kindlaks on määratud, millal ja kes seiret ja mõõtmist teeb ning millal tulemusi analüüsitakse ja hinnatakse.

Miile järgi seda näeb: Mõõdikute lehele lisatud sageduse ja vastutaja veerud. Korduv kalendrikohtumine hindamiseks tõendab regulaarsust paremini kui ükski kirjeldus.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

9.1-4 Seire ja mõõtmise tulemusi säilitatakse dokumenteeritud teabena.

Dokument

Milles järgi seda näeb: Arhiveeritud hindamised, eksporditud juhtpaneelid või ajareana peetav mõõdikute leht. Ajaloota reaalajavaade seda nõuet ei täida.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

9.1-5 Infoturbe toimivust ja ISMS tulemuslikkust hinnatakse mõõtmistulemuste alusel.

Mille järgi seda näeb: Kirjalik hinnang, mitte üksnes arvud: trend, põhjused, tegevusvajadus. See hinnangutekst on ühtlasi sisendiks juhtkonnapoolsele ülevaatusele.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.2.1-1 Siseauditeid tehakse kavandatud sagedusega ja need annavad teavet selle kohta, kas ISMS vastab organisatsiooni enda nõuetele ja standardi nõuetele ning kas see on tulemuslikult rakendatud.

Mille järgi seda näeb: Enne sertifitseerimisauditit on lõpule viidud vähemalt üks täielik siseauditi tsükkel, mis katab kogu käsitlusala. Sellela jääb sertifitseerimine kättesaamatuks; see on esmasertifitseerimise üks sagedasemaid komistuskive.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.2.2-1 Auditiprogramm on kavandatud, kehtestatud ja ajakohasena hoitud; see määratleb sageduse, meetodid, vastutused, planeerimisnõuded ja aruandluse ning arvestab asjaomaste protsesside tähtsust ja varasemate auditite tulemusi.

Mille järgi seda näeb: Mitmeaastane auditiprogramm, mis katab sertifitseerimistsükli jooksul kõik peatükid ja kõik rakendatavad ohjemeetmed, kriitilistes valdkondades suurema sagedusega. Lihtne kolme aasta tabel on täiesti piisav.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.2.2-2 Iga auditi jaoks on määratletud auditikriteeriumid ja auditi käsitlusala.

Mille järgi seda näeb: Auditikava iga kuupäeva kohta koos kriteeriumidega (standard, sisemised poliitikad, lepingud) ja selge käsitlusala. Ühe lehekülje auditikava auditi kohta on piisav ja toimib ühtlasi aruande alusena.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.2.2-3 Audiitorid valitakse ja auditid viiakse läbi viisil, mis tagab objektiivsuse ja erapooletuse. Keegi ei auditeeri oma tööd.

Mille järgi seda näeb: Sõltumatus on siin raske lävi: kes kirjutas poliitikad ja seadistas süsteemid, see neid ei auditeeri. Väga väikeses ettevõttes tähendab see peaaegu alati väljastpoolt kaasatud siseaudiitorit, näiteks lepingulist nõustajat või kolleegi partnerettevõttest; tõendiks on auditileping ja audiitori sõltumatuse kinnitus. Ainult piisavalt suures meeskonnas saab rolli sisemiselt roteerida inimesele, kes ei vastuta auditeeritava valdkonna eest, ja see on siis rollimaatriksist näha.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.2.2-4 Audititulemustest antakse aru asjaomasele juhtkonnale.

Mille järgi seda näeb: Auditiaruanne koos leidude, mittevastavuste, soovitude ja levitusloendiga ning tõend juhtkonnale üleandmise kohta, näiteks protokollitud päevakorrapunkt või kuupäevastatud üleandmine e-kirjaga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.2.2-5 Auditiprogrammi ja auditi tulemuste kohta säilitatakse dokumenteeritud teavet.[Dokument](#)

Mille järgi seda näeb: Auditiprogramm, auditikavad, auditiaruanded ja neist tulenevad tegevused on koos ühes kohas. Seos leiu ja korrigeeriva tegevuse vahel (punkt 10.2) on algusest lõpuni nähtav.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.3.1-1

Tippjuhtkond vaatab ISMS kavandatud sagedusega üle, et tagada selle jätkuv sobivus, piisavus ja tulemuslikkus.

Mille järgi seda näeb: Vähemalt kord aastas ja ajastatud enne välisauditit. Ka väga väikeses ettevõttes on olemas kuupäevastatud ja allkirjastatud protokoll, isegi kui juhtkond ja ISMS omanik on sama isik.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-1

Juhtkonnapoolne ülevaatus käsitleb varasematest juhtkonnapoolsetest ülevaatustest tulenevate tegevuste seisu.

Mille järgi seda näeb: Protokoll algab eelmise aasta otsuste ja nende praeguse seisu järeltabeliga. Ilma selle tagasiviiteta loetakse ülevaatus mittetäielikuks.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-2

Juhtkonnapoolne ülevaatus käsitleb muutusi välistes ja sisemistes teemades, mis on ISMS seisukohalt olulised, sealhulgas kliimamuutuse asjakohaseid aspekte.

Mille järgi seda näeb: Eraldi päevakorrapunkt, mis viitab ajakohastatud kontekstianalüüsile. Kliimamuutust ei ole selle punkti tekstis otsesõnu nimetatud (Amd 1:2024 muudab üksnes punkte 4.1 ja 4.2), kuid see jõuab siia punkti 4.1 teemade muutuste kaudu ja audiitorid ootavad seda. Ka tulemus, et teema ei ole oluline ja on muutumatu, kuulub protokollis.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-3

Juhtkonnapoolne ülevaatus käsitleb muutusi huvipoolte vajadustes ja ootustes, mis on ISMS seisukohalt olulised.

Mille järgi seda näeb: Uued kliendinõuded lepingutest ja turbeküsimustikest, uued õiguslikud kohustused, sertifitseerimisasutuse nõuded. Need on protokollis loendina koos allikatega.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-4

Juhtkonnapoolne ülevaatus käsitleb tagasisidet infoturbe toimivuse kohta, sealhulgas mittevastavusi ja korrigeerivaid tegevusi, seire ja mõõtmise tulemusi, auditi tulemusi ning infoturbe eesmärkide täitmist.

Mille järgi seda näeb: Neid nelja plokki käsitletakse eraldi päevakorrapunktidena, muidu jääb hiljem üks neist protokollist puudu. Mõõdikute leht, auditiaruanne ja eesmärkide leht on lisadena juurde pandud.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-5

Juhtkonnapoolne ülevaatus käsitleb huvipoolte tagasisidet.

Mille järgi seda näeb: Turbega seotud kliendikaebused, kliendiauditite tulemused, teated rikkumisest teavitamise kanalist, teenusepakujate tagasiside. See on protokollis kirjas ka siis, kui tulemus on, et tagasisidet ei laekunud.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-6

Juhtkonnapoolne ülevaatus käsitleb riskihindamise tulemusi ja riskikäsitlemise plaani seisu.

Mille järgi seda näeb: Kehtiv riskiregister ja käsitlemise plaani elluviimise seis on juurde pandud koos riskiomanike selgesõnalise kinnitusega jääkriski aktsepteerimise kohta.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

9.3.2-7 Juhtkonnapoolne ülevaatus käsitleb pideva parendamise võimalusi.

Mille järgi seda näeb: Päevakorrapunkt konkreetsete parendusideedega ja otsusega iga idee kohta. Vastuvõetud ideed liiguvad parendusregistrisse kannetena koos tähtaegadega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.3.3-1 Juhtkonnapoolse ülevaatus tulemused sisaldavad otsuseid pideva parendamise võimaluste ja ISMS muutmise vajaduse kohta.

Mille järgi seda näeb: Protokoll lõpeb otsuste jaotisega: otsus, vastutaja, tähtaeg. Otsusteta protokoll on auditis leid, sest siis puudub eestvedamise mõju.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

9.3.3-2 Juhtkonnapoolse ülevaatus tulemuste tõendina säilitatakse dokumenteeritud teavet.[Dokument](#)

Mille järgi seda näeb: Allkirjastatud protokoll koos kuupäeva, osalejate, sisendite, hinnangu ja otsustega. See on üks esimesi dokumente, mida sertifitseerimisasutus 1. etapis küsib.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10 Parendamine**7****10.1-1 ISMS sobivust, piisavust ja tulemuslikkust parendatakse pidevalt.**

Mille järgi seda näeb: Parendusregister, mida toidavad mitu allikat (auditid, juhtumid, ideed, mõõdikute kõrvalekaldeid) ja milles on aja jooksul nähtav edenemine. Tõendiks on järjepidevus mitme kuu ulatuses, mitte kannete arv.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10.2-1 Mittevastavuse ilmnemisel reageerib organisatsioon sellele: ta ohjab ja parandab seda ning tegeleb tagajärgedega.

Mille järgi seda näeb: Mittevastavuse teade koos kohese tegevuse ja kuupäevaga. Allikad on siseauditid, välsauditid, juhtumid ja tähelepanekud igapäevatööst; kõik need toidavad sama registrit.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10.2-2 Hinnatakse, kas põhjuste kõrvaldamiseks on tegevust vaja, et mittevastavus ei korduks ega ilmneks mujal; see hõlmab kontrolli, kas sarnaseid mittevastavusi esineb või võiks esineda.

Mille järgi seda näeb: Algpõhjuse analüüs on dokumenteeritud, näiteks 5 korda miks või Ishikawa abil, koos selgesõnalise seisukohaga ülekantavuse kohta teistele süsteemidele või protsessidele. Ülekantavuse samm jäetakse kõige sagedamini vahele.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10.2-3 Vajalikud korrigeerivad tegevused viiakse ellu ja nende tulemuslikkus vaadatakse üle.

Mille järgi seda näeb: Iga tegevuse juures on registreeritud elluviimise kuupäev, tõendi artefakt ja hilisem tulemuslikkuse ülevaatus koos oma kuupäevaga. Kaks kuupäevavälja rea kohta on lihtsaim viis tulemuslikkuse ülevaatus mitte kaotada.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10.2-4 **Vajaduse korral tehakse mittevastavuse tulemusena ISMS muudatusi.**

Mille järgi seda näeb: Kui mittevastavus taandub lüngale poliitikas, riskiregistris või SoA-s, siis on muudatus seal nähtav. Viide mittevastavuselt ajakohastatud dokumendi versioonile sulgeb ahela.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10.2-5 **Korrigeerivad tegevused vastavad esinenud mittevastavuste mõjule.**

Mille järgi seda näeb: Registris on raskusastme hinnang, millest nähtub tegevuse proportsionaalsus. Ei tühiseid asju projektina ega tõsiseid kõrvalekaldeid pelga meeldetuletuskirjaga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

10.2-6 **Mittevastavuste laadi, nende suhtes võetud tegevuste ja korrigeerivate tegevuste tulemuste kohta säilitatakse dokumenteeritud teavet.**[Dokument](#)

Mille järgi seda näeb: Mittevastavuste ja korrigeerivate tegevuste register veergudega laad, põhjus, tegevus, vastutaja, tähtaeg ja tulemuslikkuse ülevaatuse tulemus. See on kohustuslik tõend ja seda võetakse ette igal järelevalveauditiil.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5 Lisa A: Korralduslikud ohjemeetmed

37

A.5.1 **Infoturbe poliitikad: Üldine infoturbepoliitika ja teemapõhised poliitikad on määratletud, juhtkonna kinnitatud, kommunikeeritud ning vaadatakse üle kavandatud sagedusega ja alati, kui toimuvad olulised muudatused.**[Dokument](#)

Mille järgi seda näeb: Poliitikate kogum koos versiooni, kinnitamise kuupäeva ja järgmise ülevaatuse kuupäevaga ning tõend tutvumise kohta. Väikeses ettevõttes piisab raampoliitikast ja käputäiest teemapoliitikatest (pääs, krüptograafia, kaugtöö, juhtumid).

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.2 **Infoturbe rollid ja vastutused: Infoturbe rollid ja vastutused on määratletud ja jaotatud vastavalt organisatsiooni vajadustele.**

Mille järgi seda näeb: Rollimaatriks nimede, asendajate ja ülesannetega. Väga väikeses ettevõttes on avalikult välja öeldud, kus mitu rolli koondub ühele inimesele, ja see on seotud punkti A.5.3 kompenseerivate ohjemeetmetega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.3 **Kohustuste lahusus: Kohustused ja vastutusosalad, mis on mõeldud teineteist kontrollima, ei ole ühe inimese käes. Eesmärk on, et keegi ei saa muudatust üksi algatada, heaks kiita ja varjata.**

Mille järgi seda näeb: Väikeses ettevõttes on täielik lahusus struktuurselt võimatu; üldsõnaline väide vastavuse kohta variseb auditi vestluses kohe kokku. Kindla aluse annab aus analüüs: millised kohustuste kombinatsioonid on kriitilised (arendada ja välja lasta, õigusi anda ja neid kasutada, makseid algatada ja heaks kiita), millised neist on ühe inimese käes ja millised kompenseerivad ohjemeetmed kehtivad. Toimivad lahendused on muutumatud auditilogid, mis on kolmandale poolele kättesaadavad, MFA privilegeeritud kontodel, automaatsed CI väravad ja harude kaitse nelja silma ülevaatuse asemel, välise inimese tehtav perioodiline logide ülevaatus ning eraldi heakskiit maksetele. Analüüs ja kompenseerivad ohjemeetmed on omaette kuupäevastatud dokumendis ja sellele on viidatud SoA-st.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.4 **Juhtkonna vastutused: Juhtkond nõuab kogu personalilt infoturbe rakendamist kooskõlas kehtestatud poliitikate ja korraga.**

Mille järgi seda näeb: Kohustus töö- ja töövõtulepingutes, poliitikatega tutvumise kinnitus sisseelamisel ning juhtkonna regulaarsed meeldetuletused. Tõendiks on allkirjastatud kohustuste kinnitused ja koosolekuprotokollid.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.5 Kontakt asutustega: Asjakohaste asutustega hoitakse sobivaid kontakte ja nendeni jõuab vajaduse korral.

Mille järgi seda näeb: Kontaktide loend, kus on pädev andmekaitseasutus, politsei või küberkuritegevuse üksus, riiklik küberturbe teavituspunkt ja NIS2 teavituskanalid, kui need kuuluvad käsitusallas. Tähtajad (näiteks 72 tundi GDPR alusel) on kirjas otse loendis.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.6 Kontakt erialarühmadega: Kontakte erialarühmade, turbefoorumite ja kutseühendustega hoitakse.

Mille järgi seda näeb: Liikmesused, tellitud teavitus (riiklik CERT, tootjate vood), osalemine erialarühmades. Lihtne tõend: tellimuste loend ja üks näide selle kohta, kuidas teavitus viis tegevuseni.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.7 Ohuteave: Teavet infoturbe ohtude kohta kogutakse ja analüüsitakse, et sellest sobivad tegevused tuletada.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Väikesele ettevõttele jõukohane: tellida riikliku CERT-i ja tootjate teavitusd ning teha lühike igakuine ülevaatus koos asjakohasuse otsuse ja sellest tuletatud piletitiga. Tõendiks on analüüs, mitte tellimus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.8 Infoturbe projektijuhtimises: Infoturbe on lõimitud projektijuhtimisse sõltumata projekti liigist.

Mille järgi seda näeb: Turbepunktid projekti kontroll-lehel: kaitsevajadus, riskide ülevaatus, andmekaitse kontroll, turbe heakskiit enne käikuandmist. Agiilsetes meeskondades on need kinnistatud püsipunktidenä tööks valmiduse ja valmis töö kriteeriumides.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.9 Teabe ja muude seotud varade loend: Teabe ja muude seotud varade loend koos nimeliste omanikega on koostatud ja seda hoitakse ajakohasena.

Mille järgi seda näeb: Varade loend, mis katab riistvara, tarkvara, pilveteenused, andmehoidlad, domeenid ja kontod, igaühel omanik ja kaitsevajadus. Väikeses ettevõttes saab selle koostada automaatselt MDM väljavõttest, litsentside loendist ja pilvekonsoolist; ajakohane kuupäev on kohustuslik.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.10 Teabe ja muude seotud varade lubatud kasutus: Teabe ja muude seotud varade lubatud kasutuse ja käitlemise reeglid on tuvastatud, dokumenteeritud ja rakendatud.[Dokument](#)

Mille järgi seda näeb: Lubatud kasutuse poliitika seadmetele, võrkudele, pilvekontodele ja tehisintellekti (AI) tööriistadele koos tutvumise kinnitusega. Isiklikud seadmed ja välised tehisintellekti teenused on selgesõnaliselt kaetud, sest just seal lekitab kõige rohkem.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.11 Varade tagastamine: Töösuhte lõppemisel või muutumisel on reguleeritud ja kirjalikult kinnitatud, et kõik väljastatud seadmed, võtmed, kontod ja dokumendid tagastatakse.

Mille järgi seda näeb: Lahkumise kontroll-leht koos tagastuskinnitusega sülearvuti, autentimisvahendite, võtmete, sertifikaatide ja andmekandjate kohta ning kontode sulgemine samal päeval. See kehtib täpselt samuti vabakutseliste ja praktikantide kohta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.12 Teabe liigitamine: Teave on liigitatud vastavalt selle kaitsevajadusele konfidentsiaalsuse, tervikluse, käideldavuse ja õiguslike nõuete osas.

Mille järgi seda näeb: Lihtne skeem kolme või nelja tasemega (avalik, sisemine, konfidentsiaalne, rangelt konfidentsiaalne) ja konkreetsed käitlemisreeglid iga taseme kohta. Määrangud on kirjas varade loendis või isikuandmete töötlemise toimingute registris.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.13 Teabe märgistamine: Liigitustase on äratuntav dokumendil, failil või sõnumil endal, nii et saajad teavad selle käitlemist ilma järele küsimata.

Mille järgi seda näeb: Märgistus dokumendi päises, faili nimes, e-kirja teemareal või tundlikkuse siltidega pilvekontoripaketis. Tõendiks on näidised tegelikult märgistatud dokumentidest, mitte üksnes reegel.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.14 Teabe edastamine: Reeglid, kord ja kokkulepped teabe edastamiseks organisatsiooni sees ja väliste pooltega on olemas.

Mille järgi seda näeb: Reegel, mis ütleb, milline kanal on lubatud millise liigitustaseme jaoks: krüpteeritud e-kiri või andmeruum konfidentsiaalse sisu jaoks, saatmine isiklike sõnumirakendustega välistatud. Konfidentsiaalsed edastused on tagatud konfidentsiaalsuslepingutega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.15 Pääsu ohjamine: Reeglid füüsilise ja loogilise pääsu ohjamiseks teabele ja muudele seotud varadele on kehtestatud ja rakendatud äri- ja turbenõuete alusel.

Mille järgi seda näeb: Pääsu ohjamise poliitika, mis järgib teadmisyajaduse ja vähimate õiguste põhimõtet, koos rollide ja õiguste kaardistusega. Tõendiks on õiguste tegelik seadistus identiteedipakkujas, mitte poliitika üksi.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.16 Identiteedihaldus: Identiteetide kogu olelusringi hallatakse.

Mille järgi seda näeb: Protsess loomisest muutmise kaudu sulgemiseni, eelistatavalt koondatud identiteedipakkujasse koos ühekordse sisselogimisega. Jagatud rühmakontosid ei ole; kus need on tehniliselt vältimatud, on konto nimetatud, põhjendatud ja selle kasutus logitud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.17 Autentimisteave: Autentimisteabe jagamist ja haldust ohjab haldusprotsess, mis nõuab inimestelt selle nõuetekohast käitlemist.

Mille järgi seda näeb: Paroolihaldur kohustusliku tööriistana, poliitika parooli kvaliteedi ja MFA kohta, turvaline esmane pääs ja lähtestamise kord koos isiku tuvastamisega. Tõendiks on seadistuse ekraanipildid ja paroolihalduri aruanne.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.18 Pääsuõigused: Pääsuõigusi antakse, vaadatakse üle, muudetakse ja eemaldatakse kooskõlas pääsu ohjamise poliitikaga.

Mille järgi seda näeb: Perioodiline pääsuõiguste ülevaatus vähemalt kord aastas koos dokumenteeritud tulemusega konto kohta ja tõendiga eemaldatud õiguste kohta. Õiguste eemaldamine lahkumise päeval on koht, mida audiitorid meelsasti konkreetse juhtumi kaudu järele kontrollivad.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.19 Infoturve tarnijasuhetes: Protsessid ja kord kolmandate poolte toodete ja teenuste kasutamisest tulenevate turberiskide juhtimiseks on määratletud ja rakendatud.

Mille järgi seda näeb: Tarnijate loend koos kriitilisuse taseme ja hindamise sügavusega. Kriitiliste tarnijate puhul kogutakse tõendeid (ISO 27001 sertifikaat, SOC 2 aruanne) omaenda auditite tegemise asemel, mis on väikese ettevõtte jaoks ainus realistlik tee.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.20 Infoturbe käsitlemine tarnijalepingutes: Asjakohased turbenõuded on iga tarnijaga kokku lepitud ja lepingutes kirja pandud.

Mille järgi seda näeb: Infoturbe lepingulisa koos juhtumitest teavitamise kohustuste, alltöötajate reeglite, kustutamiskohustuste ja audititõigustega. Standardteenuste puhul piisab tarnija tingimustest ja andmetöötluslepingust, kui nende sisu on üle vaadatud ja dokumenteeritud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.21 Infoturbe juhtimine IKT tarneahelas: Protsessid info- ja kommunikatsioonitehnoloogia tarneahela turberiskide juhtimiseks on määratletud ja rakendatud.

Mille järgi seda näeb: See hõlmab tarkvarasõltuvusi ja tarnijate endi alltarnijaid. Praktikaks: tarkvara koostisosade loend (SBOM) või sõltuvuste loend, automaatne haavatavate pakettide kontroll CI-s ja tarkvara hankimine üksnes allkirjastatud või ametlikest kanalitest.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.22 Tarnijateenuste seire, ülevaatus ja muudatuste haldus: Tarnijateenuste muutusi seiratakse, vaadatakse üle ja hallatakse regulaarselt.

Mille järgi seda näeb: Iga-aastane tarnijate ülevaatus, mis vaatab juhtumeid, käideldavuse aruandeid ja sertifikaatide kehtivust, ning kanal tarnija muudatusteadete jaoks. Tulemus on kirja pandud lühikese märkmena tarnija kohta.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.23 Infoturve pilveteenuste kasutamisel: Protsessid pilveteenuste hankimiseks, kasutamiseks, haldamiseks ja neist väljumiseks on kehtestatud kooskõlas turbenõuetega.

Mille järgi seda näeb: Uus 2022. aasta väljaandes ja keskne ohjemeede väikeste pilvepõhiste ettevõtete jaoks. Tõendiks on pilvepoliitika koos uute teenuste heakskiitmise protsessiga, dokumenteeritud jagatud vastutuse mudel teenuse kohta, turvakarastuse seaded ja väljumisstrateegia koos andmete tagastamise ja kustutamise kinnitusega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.24 Infoturbe juhtumite halduse planeerimine ja ettevalmistus: Protsessid, rollid ja vastutused juhtumite käsitlemiseks on kavandatud ja kehtestatud.[Dokument](#)

Mille järgi seda näeb: Juhtumitele reageerimise plaan koos teavitustega, rollide, eskaleerimistasemete, tööväliste kontaktide ja kommunikatsioonimallidega. Väikesele meeskonnale realistlik: üks lehekülg, aga läbi harjutatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.25 Infoturbe sündmuste hindamine ja otsustamine: Turvasündmusi hinnatakse ja otsustatakse, kas need liigitatakse infoturbe juhtumiteks.

Mille järgi seda näeb: Triaaži kriteeriumid koos raskusastme maatriksiga ja sündmuste register, milles on põhjendusega kirjas ka kõrvale jäetud sündmused. Eristus sündmuse ja juhtumi vahel on registris nähtav.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.26 Reageerimine infoturbe juhtumitele: Juhtumeid käsitletakse kooskõlas dokumenteeritud korraga.

Mille järgi seda näeb: Juhtumitoimikud koos ajajoone, võetud tegevuste, kaasatud inimeste ja sulgemisotsusega. Kui tegelikku juhtumit veel olnud ei ole, on parim olemasolev tõend dokumenteeritud lauaharjutus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.27 Infoturbe juhtumitest õppimine: Juhtumitest saadud teadmisi kasutatakse turbe ohjemeetmete tugevdamiseks.

Mille järgi seda näeb: Süüdistusteta juhtumijärgne ülevaatus koos algpõhjuse analüüsi ja sellest tuletatud tegevustega, seotud parendusregistriga ja vajaduse korral riskiregistriga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.28 Tõendite kogumine: On reguleeritud, kuidas turvasündmusega seotud jäljed tuvastatakse, kindlustatakse ja säilitatakse, nii et need jäävad hiljem kasutatavaks.

Mille järgi seda näeb: Lühike tõendite säilitamise kord: süsteeme ei ehitata enneaegselt üles, tömmised ja logid kindlustatakse, valdusahel dokumenteeritakse. Väikesele ettevõttele piisab, kui on määratletud raskusaste, millest alates kaasatakse väline kohtuekspertiisi pakkuja, koos kontaktandmetega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.29 Infoturbe häire ajal: Organisatsioon kavandab, kuidas infoturvet häire ajal sobival tasemel hoitakse.

Mille järgi seda näeb: Hädaolukorra lahendused ei lülita turvet välja. Dokumenteeritud on, et MFA, logimine ja pääsupiirangud kehtivad ka varutalitluses ning et hädaolukorra kontod (break-glass kontod) on pitseeritud, dokumenteeritud ja hiljem üle vaadatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.30 IKT valmisolek talitluspidevuseks: IKT valmisolek on kavandatud, rakendatud, ajakohasena hoitud ja testitud talitluspidevuse eesmärkide ja IKT pidevuse nõuete alusel.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Tõendiks on määratletud taasteaja eesmärgid (RTO) ja taastepunkti eesmärgid (RPO) iga kriitilise süsteemi kohta, taastamise kord ja vähemalt üks dokumenteeritud test aastas. Õnnestunud taastamise test koos kuupäeva ja kestusega on kõige tugevam üksik tõend.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.31 Õiguslikud, seadusest tulenevad, regulatiivsed ja lepingulised nõuded: Asjakohased nõuded ja nende täitmise viis on tuvastatud, dokumenteeritud ja hoitakse ajakohasena.[Dokument](#)

Mille järgi seda näeb: Õigusaktide register, mis katab GDPR-i, sideõiguse, äri- ja maksuõiguse ning kohalduvuse korral NIS2 või valdkonnapõhised reeglid, igapäev juures seda rakendav reegel ja ülevaatus kuupäev. Iga-aastane ülevaatus on piisav, kuid see on kuupäevastatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.32 Intellektuaalomandi õigused: Asjakohane kord intellektuaalomandi õiguste kaitseks on rakendatud.

Mille järgi seda näeb: Kasutatava tarkvara litsentside loend, avatud lähtekoodi litsentside kontroll tootes (litsentsiskanner CI-s) ja reegel kolmanda poole koodi ning genereeritud koodi käsitlemiseks. Tõendiks on koostest (build) saadav litsentsiaruanne.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.33 Kirjete kaitse: Äri- ja tõenduslikud kirjed on hoiul nii, et need ei saa kaotsi minna, neid ei saa märkamatuks muuta ega saa need sattuda valesse kätte, ja see kehtib kogu säilitustähtaja jooksul.

Mille järgi seda näeb: Säilitusplaan koos seadusjärgsete tähtaegadega, muutmiskindel hoiustamine, piiratud pääs ja varukoopia. Maksuga seotud kirjete juures on seadusjärgsed säilitustähtjad selgesõnaliselt nimetatud, sest audiitorid kontrollivad meelsasti just seda.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.34 Eraelu puutumatus ja PII kaitse: Eraelu puutumatus ja isikuandmete (PII) kaitse nõuded on tuvastatud ja täidetud kooskõlas kohalduva õigusega.

Mille järgi seda näeb: Isikuandmete töötlemise toimingute register, andmetöötluslepingud, kustutamise kontseptsioon, andmesubjekti õiguste protsess ja nõude korral andmekaitsealane mõjuhindang. Sidumine ISMS-iga ühise varade loendi kaudu hoiab ära topelthalduse.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.35 Infoturbe sõltumatu ülevaatus: Organisatsiooni infoturbe juhtimise lähenemine vaadatakse sõltumatult üle kavandatud sagedusega ja alati, kui toimuvad olulised muudatused.

Mille järgi seda näeb: Tõendiks on sõltumatu audiitori tehtud siseaudit, välised läbistustestid või sertifitseerimisaudit ise. Sõltumatu tähendab, et seda ei tee inimene, kes vastutab ülevaadatava valdkonna eest.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.36 Infoturbe poliitikate, reeglite ja standardite järgimine: Organisatsiooni enda turbepoliitikate ja kohalduvate reeglite järgimist vaadatakse regulaarselt üle.

Mille järgi seda näeb: Vastavuskontrollid koos kuupäeva ja tulemusega, näiteks seadistuse võrdlus omaenda turvakarastuse lähtetasemega, dokumentide märgistuse pisteline kontroll, automaatsed poliitikakontrollid pilves. Kõrvalekalded liiguvad korrigeerivate tegevuste registrisse.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.5.37 Dokumenteeritud käitamiskord: Teabetöötlusrajatiste käitamiskord on dokumenteeritud ja tehtud kättesaadavaks inimestele, kes seda vajavad.[Dokument](#)

Mille järgi seda näeb: Tegevusjuhendid varukoopia ja taastamise, juurutuse, kasutajate halduse, paikamise ja juhtumite käsitlemise kohta. Lühike ja ajakohane kaalub üles mahuka ja aegunu; viimase muutmise kuupäev iga juhendi juures on kohustuslik.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6 Lisa A: Inimestega seotud ohjemeetmed

8

A.6.1 Taustakontroll: Kandidaate, kes hakkavad organisatsiooni heaks töötama, kontrollitakse eelnevalt seaduse piires ja kaitsevajadusega proportsionaalselt; tundlike rollide puhul korraldatakse kontrolli töösuhte kestel.

Mille järgi seda näeb: Töötajate puudumisel saab selle ohjemeetme põhjendada praegu mitterakendatavana, kuid kord palkamise juhiks on siiski määratletud ja rakendatavuse avalduses kavandatavana kirjas. Jõukohane maht: isikusamasuse, elulookirjelduse ja soovijate kontroll ning tunnistused; karistusregistri päring üksnes siis, kui kaitsevajadus seda õigustab ja seadus lubab. Sama tase on vabakutselistelt ja lepingupartneritelt nõutud lepingutega, muidu avaneb lünk just seal.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.2 Töösuhte tingimused: Lepingulised kokkulepped sätestavad töötajate ja organisatsiooni infoturbe vastutused.

Mille järgi seda näeb: Turbeklausel töö- või teenuslepingus koos viitega kohalduvatele poliitikatele. Vabakutseliste puhul sama klausel teenuslepingus ja lisaks konfidentsiaalsusleping.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.3 Infoturbe teadlikkus, haridus ja koolitus: Töötajad ja asjakohased välised pooled saavad sobiva teadlikkuse ja koolituse ning regulaarsed uuendused organisatsiooni poliitikate kohta.

Mille järgi seda näeb: Iga-aastane koolitus koos osalemise tõendi ja kuupäevaga, täiendatud andmepüügi simulatsioonidega, mille klikimäär on hinnatud. Ka üksi tegutsev ettevõtja vajab tõendit oma täiendõppe kohta, näiteks kursuste kinnitusi.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.4 Distsiplinaarmenetlus: Ametlik ja kommuniqueeritud menetlus on olemas nende inimeste suhtes meetmete võtmiseks, kes on turbepoliitikaid rikkunud.

Mille järgi seda näeb: Töötajate puudumisel saab selle põhjendada praegu mitterakendatavana, kuid menetlus on siiski palkamise juhuks määratletud; ära langeb üksnes selle kohaldamine, mitte reegel. Nõutav on astmeline ja kommuniqueeritud reageeringute skaala (vestlus, märkus, hoiatus, lepingu lõpetamine) kooskõlas tööõiguse ja töötajate esindamise reeglitega. Lepingupartnerite puhul kajastub sanktsioonitase lepingus, näiteks leppetrahvi või ülesütlemisõigusena.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.5 Vastutused pärast töösuhte lõppemist või muutumist: Turbevastutused ja kohustused, mis jäävad kehtima pärast töösuhte lõppu või rollimuutust, on määratletud, jõustatud ja asjaomastele inimestele kommuniqueeritud.

Mille järgi seda näeb: Lahkumise kontroll-leht koos õiguste eemaldamise, varade tagastamise, üleandmise ja selgesõnalise meeldetuletusega kehtivate konfidentsiaalsuskohustuste kohta. Allkirjastatud lahkumisvestluse kirje on lihtsaim tõend.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.6 Konfidentsiaalsus- või saladuse hoidmise lepingud: On kindlaks määratud, kes konfidentsiaalsuslepingu allkirjastab. Sisu vastab teabe kaitsevajadusele, lepingud on allkirjastatud, arhiveeritud ja neid vaadatakse regulaarselt üle, et need ajakohasena hoida.

Mille järgi seda näeb: Allkirjastatud konfidentsiaalsuslepingud töötajatele, vabakutselistele, teenusepakkujatele ja praktikantidele koos kehtivusajaga pärast suhte lõppu. Ülevaattetabel lepingupoole, kuupäeva ja kehtivusega muudab portfelli auditeeritavaks.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.7 Kaugtöö: Turbemeetmed on rakendatud seal, kus inimesed töötavad väljaspool organisatsiooni ruume ja pääsevad seejuures organisatsiooni teabele.

Mille järgi seda näeb: Kodukontori ja kaugtöö poliitika koos nõuetega ketta krüpteerimise, ekraaniluku, turvalise Wi-Fi, VPN või zero trust pääsu kasutamise, privaatsusfiltri ja isiklike seadmete heakskiiduta kasutamise keelu kohta. Tõendiks on lõppseadmete MDM vastavusaruanne.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.6.8 Infoturbe sündmustest teavitamine: Olemas on mehhanism, mille kaudu inimesed saavad märgatud või kahtlustatavatest turvasündmustest õigel ajal teada anda.

Mille järgi seda näeb: Selgelt kommuniqueeritud teavituskanal (postkast, vestluskanal, telefoninumber) koos kinnitusega, et heauskse teavituse eest sanktsioone ei järgne. Tõendiks on teavituste hulk sündmuste registris; püsivalt tühi register on auditis hoiatusmärk.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7 Lisa A: Füüsilised ohjemeetmed

14

A.7.1 Füüsilise turvalisuse piirid: Turvapiirid on määratletud ja kasutusel, et kaitsta alasid, kus on teave ja teabetöötlusrajaajad.

Mille järgi seda näeb: Piiride kirjeldus koos joonise või fotodega: hoone, kontor, serverikapp. Kodukontoris on piiriks lukustatav tööruum või selle puudumisel lukustatav kapp; see on pigem kirjeldatud kui välja jäetud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.2 Füüsiline sissepääs: Turvaaladid kaitstakse sobivate sissepääsu ohjemeetmete ja pääsupunktidega.

Mille järgi seda näeb: Võtmete või kaartide register koos väljastamise ja tagastamisega ning külastajate reegel koos saatmise ja logiga. Kui kasutatakse jagatud kontorit või andmekeskust, võetakse tõendiks käitaja sissepääsu ohjemeetmed ja need kinnistatakse lepinguga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.3 Kontorite, ruumide ja rajatiste turvamine: Kontorite, ruumide ja rajatiste füüsiline turvalisus on kavandatud ja rakendatud.

Mille järgi seda näeb: Lukustatavad uksed, akende kaitse esimesel korrusel, konfidentsiaalsed ekraanid väljastpoolt nähtamatud, tundlikel aladel ilma ettevõtte sildita. Tõendiks piisab lühikesest kirjeldusest ja fotost.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.4 Füüsilise turvalisuse seire: Rume seiratakse pidevalt volitamata füüsilise pääsu suhtes.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Võimalused on valvesüsteem, liikumisandurid, videovalve või sissepääsulogid. Videovalve puhul on andmekaitse vastavus kontrollitud; kodukontoris on põhjendatud alternatiiviks valvesüsteemi, lukustatud ruumi ja selle tõdemuse kombinatsioon, et tundlikke servereid seal ei hoita.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.5 Kaitse füüsiliste ja keskkonnaohtude vastu: Kaitse on olemas füüsiliste ja keskkonnaohtude vastu, nagu loodusõnnetused ning tahtlik või tahtmatu kahjustamine.

Mille järgi seda näeb: Tule, vee, kuumuse, elektrikatkestuse ja sissemurdumise ülevaatus koos olemasolevate meetmetega (suitsuandurid, tulekustutid, seadmed veetorude alt eemal, varukoopia teises asukohas). Siin haakub punkti 4.1 kliimamuutuse otsus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.6 Töötamine turvaaladel: Turvaaladel töötamise meetmed on kavandatud ja rakendatud.

Mille järgi seda näeb: Reeglid serveriruumi või kõrge konfidentsiaalsusega alade kohta: kolmandate poolte järelevalveta pääs välistatud, salvestamine kaamerate või mobiilseadmetega välistatud, tehtud töö logitud. Kui turvaaladid ei ole, saab seda põhjendada viitega üksnes pilves toimimisele.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.7 Puhas laud ja puhas ekraan: Reeglid puhta laua kohta paberite ja irdkandjate osas ning lukustatud ekraanide kohta on määratletud ja neid järgitakse.

Mille järgi seda näeb: See kehtib täies ulatuses ka kodukontoris ja seetõttu ei saa seda mitterakendatavaks kuulutada. Tõendiks on lühike reegel (dokumendid lukustatakse ära, ekraanilukk viie minuti järel, klepmärkmeid paroolidega ei ole) ja tehniliselt jõustatud lukk seadme poliitika kaudu, mille seadistust saab eksportida.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.8 Seadmete paigutus ja kaitse: Seadmed on paigutatud turvaliselt ja kaitstud.

Mille järgi seda näeb: Paigutus eemal läbikäigukohtadest ja avalikest aladest, väljastpoolt nähtamatu, kaitse kuumuse ja niiskuse eest, kaablilukud mobiilsetele seadmetele. Piisab lühikesest kirjeldusest kodukontori või kontori poliitikas.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.9 Väljaspool ruume asuvate varade turve: Väljaspool ruume asuvad varad on kaitstud.

Mille järgi seda näeb: Väikeses ettevõttes on need peamiselt sülearvuti, nutitelefon ja välised andmekandjad ning seda ei saa ära põhjendada. Tõendiks on jõustatud ketta krüpteerimine, MDM kaudu sisse lülitatud kaugkustutus, reegel seadmete sõidukisse jätmise ja avalike võrkude VPN-ita kasutamise vastu ning kaotuse teavitustee. Kõige kindlam üksik tõend on MDM vastavusaruanne, mis näitab krüpteerimise seisu seadme kaupa.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.10 Andmekandjad: Andmekandjaid hallatakse kogu nende olelusringi ulatuses kooskõlas liigitusskeemi ja käitlemisnõuetega, hankimisest kasutamise ja transpordi kaudu hävitamiseni.

Mille järgi seda näeb: See kehtib ka puhtalt mobiilse töö puhul, sest USB-pulgad, välised kettad ja varukoopia kandjad on olemas. Tõendiks on kandjate register, krüpteeritud kandjad, tehniliselt jõustatud keeld heakskiiduta irdkandjatele, turvaline hoiustamine lukustatavas kohas ja üleandmine punkti A.7.14 juurde olelusringi lõpus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.11 Tugitaristu: Teabetöötlusrajatised on kaitstud tugitaristu, eelkõige elektrivarustuse, rikke vastu.

Mille järgi seda näeb: Kui servereid peetakse majas, siis katkematu toite süsteem koos dokumenteeritud testiga. Üksnes pilves toimimise korral on tõendiks viide tarnija kohustustele ja reegel selle kohta, kuidas kohaliku elektri- või internetikatkestuse ajal edasi töötada (mobiilne jagamine, varuasukoht).

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.12 Kaabelduse turve: Toite-, andme- ja sidekaabeldus on kaitstud pealtkuulamise, häirete ja kahjustuste vastu.

Mille järgi seda näeb: Kui kaabeldus on oma, siis kaitse kahjustuste ja volitamata pääsu vastu jaotuspaneelidele. Väikestes kontorites ja kodukontoris on põhjendus napp, kuid see on esitatud: ruuter ja võrgupesad ei ole avalikult ligipääsetavad, kasutamata pordid on välja lülitatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.13 Seadmete hooldus: Seadmeid hooldatakse korrektselt, et tagada teabe käideldavus, terviklus ja konfidentsiaalsus.

Mille järgi seda näeb: Hoolduskava või tootja toe seis seadme kohta ja reegel kolmandate poolte tehtavate remonttööde jaoks (andmekandja eemaldatakse enne või andmed kustutatakse ning tarnijaga sõlmitakse konfidentsiaalsusleping). Toe lõppemise kuupäevi jälgitakse varade loendis.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7.14 Seadmete turvaline hävitamine või taaskasutus: Enne andmekandjat sisaldava seadme edasiandmist, müümist või utiliseerimist on kontrollitud ja registreeritud, et sellel ei ole taastatavat kaitstud andmestikku ega litsentsitud tarkvara.

Mille järgi seda näeb: See kehtib ka kodukontoris ja kasutuselt kõrvaldatud isiklike seadmete puhul, mida tööks kasutati. Tõendiks on kustutamise kirje seadme kohta koos seerianumbri, kuupäeva ja meetodiga (krüptokustutus krüpteeritud SSD-del, ülekirjutamine, füüsiline hävitamine) või tarnija hävitamistõend. Krüpteeritud seadmete puhul piisab dokumenteeritud võtme hävitamisest, kui kord on kirjeldatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8 Lisa A: Tehnoloogilised ohjemeetmed

34

A.8.1 Kasutajate lõppseadmed: Teave, mis on kasutajate lõppseadmetes salvestatud, seal töödeldud või nende kaudu kättesaadav, on kaitstud.

Mille järgi seda näeb: Turvakarastuse lähtetase iga operatsioonisüsteemi kohta, keskne haldus MDM kaudu, ketta krüpteerimine, automaatsed uuendused ja ekraanilukk. MDM vastavusaruanne koos seisuga seadme kaupa tõendab need kõik korraga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.2 Privilegeeritud pääsuõigused: Privilegeeritud pääsuõiguste andmine ja kasutamine on piiratud ja hallatud.

Mille järgi seda näeb: Kõigi administraatorikontode loend koos põhjendusega, eraldi administraatorikontod, mida igapäevatööks ei kasutata, jõustatud MFA, ajaliselt piiratud õiguste tõstmine seal, kus võimalik, ja perioodiline ülevaatus. Väikeses ettevõttes on see punkti A.5.3 kõige tähtsam kompenseeriv ohjemeede.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.3 Teabele pääsu piiramine: Pääs teabele ja muudele seotud varadele on piiratud kooskõlas kehtestatud pääsu ohjamise poliitikaga.

Mille järgi seda näeb: Õiguste kontseptsioon, mis põhineb rollidel ja rühmadel, mitte üksikutele õiguste andmistel, tõendatuna rühmaliikmesuste väljavõttega. Pilvesalvestuse avalikud jagamislingid vaadatakse regulaarselt üle ja lastakse aeguda.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.4 Pääs lähtekoodile: Lugemis- ja kirjutuspääs lähtekoodile, arendustööriistadele ja tarkvarateekidele on asjakohaselt hallatud.

Mille järgi seda näeb: Hoidla õigused rolli järgi, kaitstud põhiharud, jõustatud ülevaatused või jõustatud olekukontrollid, otsene tõukamine põhiharusse välistatud. Tõendiks on harude kaitse seadistus ja organisatsiooni liikmete loend.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.5 Turvaline autentimine: Turvalise autentimise tehnoloogiad ja kord on rakendatud pääsupiirangute ja teemapõhise poliitika alusel.

Mille järgi seda näeb: MFA kogu välise pääsu ja kõigi administraatorikontode puhul, andmepüügikindlad meetodid (pääsuvõtmed, FIDO2) seal, kus võimalik, ja konto lukustus ebaõnnestunud katsete järel. Tõendiks on identiteedipakkuja MFA katvuse aruanne.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.6 Võimsuse haldus: Salvestusruumi, arvutusvõimsust, ribalaiust ja litsentse seiratakse ning vajadust kohandatakse piisavalt varakult, et kitsaskohad ei ohustaks kunagi käideldavust.

Mille järgi seda näeb: Salvestusruumi, arvutuskooormuse, litsentsikvootide ja pilve-eelarve seire koos lävendihoiatustega. Väikeses ettevõttes piisab hoiatusest kettakasutuse ja kulupiiride kohta ning iga-aastasest võimsuse ülevaatuselt.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.7 Kaitse pahavara vastu: Tehnilised kaitseid pahavara vastu on aktiivsed ja ajakohased ning seadmeid kasutavad inimesed on piisavalt koolitatud, et neid kaitseid mitte nurjata.

Mille järgi seda näeb: Aktiivne lõppseadmete kaitse koos keske seisuülevaatega, e-posti filter, mis kontrollib manuseid ja linke, ning reegel heakskiiduta tarkvara käivitamise vastu. Otsene tõend on kaitsevahenduse kuupäevastatud seisuaruanne.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.8 Tehniliste haavatavuste haldus: Organisatsioon saab aktiivselt teada kasutatava tehnoloogia haavatavustest, otsustab iga leiu puhul, kui avatud organisatsioon sellele on, ja sulgeb lünga määratletud tähtaegade jooksul või põhjendab teistsugust reageeringut.

Mille järgi seda näeb: Haavatavuste haldus koos allikaga (skanner, sõltuvuste kontroll CI-s, tootjate teavitused), raskusastme hinnanguga ja määratletud tähtaegadega taseme kohta, näiteks kriitiline 7 päeva jooksul. Tõendiks on skanniaruanded mitmest ajahetkest, mis näitavad avatud leidude vähenemist.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.9 Konfiguratsioonihaldus: Riistvara, tarkvara, teenuste ja võrkude konfiguratsioonid, sealhulgas turbekonfiguratsioonid, on kehtestatud, dokumenteeritud, rakendatud, seiratud ja üle vaadatud.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Tõendiks on dokumenteeritud lähtekonfiguratsioonid (turvakarastuse lähtetasemed) ja nende jõustamine, eelistatavalt taristuna koodis versioonihalduses või MDM profiilide kaudu. Triivi tuvastamine ja perioodiline konfiguratsioonide võrdlus teevad pildi täielikuks.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.10 Teabe kustutamine: Teabesüsteemides, seadmetes ja andmekandjatel salvestatud teave kustutatakse, kui seda enam ei vajata.

Mille järgi seda näeb: Uus 2022. aasta väljaandes ja tihedalt seotud GDPR-iga. Tõendiks on kustutamise kontseptsioon koos säilitustähtaegadega andmekategooria kaupa, tehniliselt rakendatud säilituspoliitikad pilveteenustes ja andmebaasides ning kustutamislõigud. Ka varukoopiad ja logiarhiivid vajavad säilitustähtaega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.11 Andmete maskeerimine: Andmete maskeerimist rakendatakse kooskõlas pääsu ohjamise teemapõhise poliitikaga ning äriliste ja õiguslike nõuetega.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Praktikas: tootmisandmeid test- ja arenduskeskkondades ei ole, nende asemel anonüümited või sünteetilised andmed; pseudonüümimine analüütikas; kontonumbrite ja juurdepääsuandmete maskeerimine logides ja tugiliides. Tõendiks on skript või kord, mis testandmed loob.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.12 Andmelekke tõkestamine: Andmelekke tõkestamise meetmeid rakendatakse süsteemidele, võrkudele ja seadmetele, mis töötlevad, salvestavad või edastavad tundlikku teavet.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Väikeses ettevõttes realistlik: pilvesalvestuse jagamislinkide ohjamine, heakskiiduta irdkandjate blokeerimine, reeglid isiklikesse postkastidesse edasisaatmise vastu, konfidentsiaalsete andmete välisesse tehisesintellekti teenustesse sisestamise kontroll ja saladuste skannimine lähtekoodis. Tõendiks on seadistus ja tabamuste ülevaatused.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.13 Teabe varundamine: Andmetest, tarkvarast ja süsteemidest on varukoopiad määratletud reegli järgi (ulatus, sagedus, säilitamine, asukoht) ja nendest taastamist ka tegelikult testitakse kindla sagedusega.

Mille järgi seda näeb: Varunduspoliitika koos sageduse, säilitamise ja väliskoopiaga 3-2-1 põhimõtte järgi, varukoopiate krüpteerimine ja kaitse lunavara ülekirjutuste vastu (muutumatud varukoopiad). Otsustav on dokumenteeritud taastamise test koos kuupäeva ja tulemusega, sest testimata varukoopia loetakse auditis olematuks.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.14 Teabetöötlusrajatiste liiasus: Teabetöötlusrajatised on rakendatud piisava liiasusega, et täita käideldavuse nõudeid.

Mille järgi seda näeb: Liiasus vastab käideldavuse eesmärkidele, mitte maksimaalsele võimalikule. Tõendiks on arhitektuuri kirjeldus liiate eksemplaride või tsoonidega, varuseadmed ja põhjendatud otsus selle kohta, kus liiasus teadlikult puudub.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.15 Logimine: Turbe seisukohalt olulised tegevused jätavad jälje. Logisid luuakse, säilitatakse, kaitstakse muutmise vastu ja ka tegelikult analüüsitakse, mitte üksnes ei koguta.

Mille järgi seda näeb: Vähemalt logitakse sisselogimised ja ebaõnnestunud katsed, õiguste muudatused, administratiivsed toimingud ja pääs konfidentsiaalsetele andmetele. Logid on kaitstud muutmise vastu ja neil on määratletud säilitustähtaeg; väikeses ettevõttes on muutumatud logid ühtlasi kompensatsiooniks punkti A.5.3 kohustuste lahususe puudumisele.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.16 Seiretegevused: Vörke, süsteeme ja rakendusi seiratakse ebatavalise käitumise suhtes ning võimalike turvajuhtumite hindamiseks võetakse sobivaid meetmeid.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Jõukohane ka ilma oma turbemeeskonnata: identiteedipakkuja hoiatused võimatu reisimise ja ebaõnnestunud katsete seeriade kohta, pilveplatvormi hoiatused ebatavalise kulu või õiguste muutuste kohta, suunatud jälgitavasse postkasti koos määratletud reageerimisajaga. Tõendiks on hoiatusreeglid ja näited käsitletud hoiatustest.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.17 Kellade sünkroonimine: Kõik süsteemid, mis logisid kirjutavad, võtavad aja määratletud usaldusväärsest allikast, nii et sündmused saab süsteemide üleselt õigesse järjekorda seada.

Mille järgi seda näeb: NTP seadistus serverites ja lõppseadmetes ning ühtne ajavöönd logides (eelistatavalt UTC). Ilma sünkroonitud ajata ei ole juhtumi rekonstrueerimine punkti A.5.28 alusel usaldusväärne; tõendiks piisab seadistuse väljavõttest.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.18 Privilegeeritud abiprogrammide kasutamine: Selliste abiprogrammide kasutamine, mis suudavad süsteemi kaitsemeetmeid eirata, on piiratud ja rangelt ohjatud.

Mille järgi seda näeb: Heakskiidetud haldustööriistade loend, kohalike administraatoriõiguste piiramine, rakenduste ohjamine (lubatud loend) seal, kus võimalik, ja kasutamise logimine. Tõendiks on poliitika ja õiguste halduse seadistus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.19 Tarkvara paigaldamine tootmissüsteemidesse: Kord ja meetmed tarkvara paigaldamise turvaliseks haldamiseks tootmissüsteemides on rakendatud.

Mille järgi seda näeb: Üksnes heakskiidetud tarkvara usaldusväärsetest allikatest, paigaldus keskse jaotuse või paketi halduri kaudu, tagasipööramise tee ja eelmise versiooni säilitamine. Tõendiks on heakskiidetud tarkvara loend ja juurutuslogid.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.20 Võrkude turve: Võrkudel ja aktiivsetel võrguseadmetel on nimeline omanik, karastatud seadistus ja jälgitav reeglistik, mis määrab, milline liiklus üldse lubatud on.

Mille järgi seda näeb: Tulemüüri reeglistik, mis järgib vaikimisi keelamise põhimõtet, dokumenteeritud avatud pordid koos põhjendusega, turvaline Wi-Fi seadistus ja võrguseadmete vahetatud vaike-juurdepääsuandmed. Tõendiks on reeglistiku väljavõte ja väline portide skannimine.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.21 Võrguteenuste turve: Võrguteenuste turbemehhanismid, teenustasemed ja haldusnõuded on tuvastatud, rakendatud ja seiratud.

Mille järgi seda näeb: Iga kasutatava võrguteenuse kohta (VPN, DNS, e-post, CDN) on dokumenteeritud turbekohustused ja omaenda seadistus, sealhulgas krüpteerimine edastusel ja tarnija teenustaseme kohustused. Tõendiks on seadistuse ülevaade ja leping või teenuse kirjeldus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.22 Võrkude eraldamine: Võrk on jaotatud tsoonideks, nii et erineva kaitsevajadusega teenused, kasutajarühmad ja süsteemid ei saa üksteiseni filtreerimata jõuda.

Mille järgi seda näeb: Eraldi võrgusegmendid või VLAN-id külalistele, haldusele ja tootmisele; pilves eraldi kontod või virtuaalvõrgud koos turberühmadega. Kodukontoris on jõukohane lahendus eraldi võrk või VLAN tööseadmetele, hoituna lahus isiklikest seadmetest ja nutikodu tehnikast.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.23 Veebifiltreerimine: Pääsu välistele veebilehtedele hallatakse, et vähendada kokkupuudet pahatahtliku sisuga.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Väikese vaevaga saavutatav filtreeriva DNS-teenuse või lõppseadmete kaitstes sisalduva veebifiltri abil, koos blokeeritud kategooriate ja blokeeritud päringute logimisega. Tõendiks on filtri seadistus ja aruande väljavõte.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.24 Krüptograafia kasutamine: Siduvalt on määratletud, kus krüpteerimist rakendatakse, milliste algoritmidega ning kuidas võtmeid kogu olelusringi jooksul luuakse, hoitakse, vahetatakse ja hävitatakse.[Dokument](#)

Mille järgi seda näeb: Krüptograafia poliitika koos heakskiidetud algoritmide ja minimaalsete võtmepikkustega, krüpteerimine edastusel (TLS) ja hoiul, ning võtmehalduse kord, mis katab loomise, hoiustamise, vahetamise ja hävitamise. Tõendiks on poliitika ja võtmeteenuse või hoidla seadistus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.25 Turvalise arenduse olelusring: Reeglid tarkvara ja süsteemide turvaliseks arendamiseks on kehtestatud ja rakendatud.

Mille järgi seda näeb: Arendusprotsessi kirjeldus koos turbepuutepunktidega igas faasis: nõuded, disain, teostus, testimine, väljalase, käitamine. Väikesele meeskonnale piisab ühest leheküljest, mis viitab konkreetsetele CI väravatele ja ülevaatus kohustusele.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.26 Rakenduste turbenõuded: Rakenduste turbenõuded on arenduse ja hankimise käigus tuvastatud, spetsifitseeritud ja heaks kiidetud.

Mille järgi seda näeb: Turbenõuded selgesõnaliste punktidenä nõuete loendis või korduvkasutatava kontroll-lehena, mis tugineb näiteks levinud rakenduste turbe tõendamise standarditele. Tõendiks on turbega seotud piletid või nõuete dokumendid.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.27 Turvalise süsteemiarhitektuuri ja projekteerimise põhimõtted: Turvalise süsteemiprojekteerimise põhimõtted on kehtestatud, dokumenteeritud ja arendustegevustes rakendatud.

Mille järgi seda näeb: Dokumenteeritud põhimõtted nagu vähimad õigused, mitmekihiline kaitse, turvalised vaikeseaded, andmete minimeerimine ja zero trust lähenemine, koos nende nähtava rakendamise arhitektuuri visandites või otsuste kirjetes.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.28 Turvaline programmeerimine: Turvalise programmeerimise põhimõtteid rakendatakse tarkvaraarenduses.

Mille järgi seda näeb: Uus 2022. aasta väljaandes. Tõendiks on siduvad programmeerimisreeglid, staatiline koodianalüüs ja saladuste skannimine kohustuslike CI väravatena, kontrollitud teekide kasutamine ja dokumenteeritud koodiülevaatused. Kui kohustuste lahusus on võimatu, asendavad jõustatud automaatsed väravad nelja silma ülevaatus; see on põhjendatud ja tõendatud konveieri seadistusega.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.29 Turbetestimine arenduses ja vastuvõtul: Turbetestimise protsessid on arenduse olelusringis määratletud ja rakendatud.

Mille järgi seda näeb: Automaatsed turbetestid konveieris (sõltuvuste kontrollid, staatiline ja dünaamiline analüüs) ning perioodiline läbistustest, kui kaitsevajadus on kõrgendatud. Tõendiks on kuupäevastatud testiaruanded ja leidude jälgimine.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.30 Sisseostetud arendus: Sisseostetud arendustegevusi suunatakse, seiratakse ja vaadatakse üle.

Mille järgi seda näeb: Kui arendus on sisse ostetud, sätestatakse turbenõuded lepingus, kindlustatakse koodi omand ja ülevaatus õigus ning tehakse enne vastuvõttu koodiülevaatused ja turbetestid. Sisseostetud arenduse puudumisel on mitterakendatavus SoA-s sidusalt põhjendatud.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.31 Arendus-, test- ja tootmiskeskondade eraldamine: Arendus-, test- ja tootmiskeskonnad on eraldatud ja kaitstud.

Mille järgi seda näeb: Eraldi kontod, projektid või nimeruumid, eraldi juurdepääsuandmed ja eraldi andmestikud. Koos punktiga A.8.11 on tagatud, et tootmisandmed ei satu tootmisvälistesse keskkondadesse. Tõendiks on keskkondade ülevaade ja õiguste jaotus.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.32 Muudatuste haldus: Teabetöötlusrajatiste ja teabesüsteemide muudatustele kohaldatakse muudatuste halduse korda.

Mille järgi seda näeb: Muudatuste protsess koos taotluse, mõju hindamise, testimise, heakskiidu, elluviimise ja tagasipööramise teega. Arendusmeeskondades täidab seda punkti muudatustaotluste konveier jõustatud kontrollide ja logitud juurutustega, kui ajalugu on muutumatu.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.33 Testteave: Testteave on asjakohaselt valitud, kaitstud ja hallatud.

Mille järgi seda näeb: Põhimõte: testsüsteemides ei ole tegelikke isikuandmeid. Kui see on vältimatu, dokumenteeritakse heakskiit, maskeerimine, pääsupiirang ja kustutamine pärast testi. Tõendiks on testandmete kontseptsioon ja kustutamislõigid.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8.34 Teabesüsteemide kaitse auditi testimise ajal: Auditi testid, mis hõlmavad pääsu tootmissüsteemidele, on kavandatud ja juhtkonnaga kokku lepitud, et vältida häireid töös.

Mille järgi seda näeb: Auditi kokkulepe koos ajaakna, käsitusala, võimaluse korral üksnes lugemispääsu, auditipääsu logimise ja juhtkonna heakskiiduga. See kehtib ka läbistustestide kohta: tõendiks on kirjalik testimisvolitus koos ajaakna ja hädakontaktiga.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

ISO/IEC 27018:2025, infoturve, küberturvalisus ja privaatsuse kaitse: juhised isikuandmete (PII) kaitseks avalikes pilvedes, mis tegutsevad PII volitatud töötlejana (3. väljaanne, 2025-08)

PII kaitse avalikus pilves

36 nõuet. Selle standardi kohta akrediteeritud sertifikaati ei ole. Versioon 07/2026.

ISO/IEC 27018 ei ole juhtimissüsteemi standard, vaid juhiste kogum, mis lisab standardile ISO/IEC 27002:2022 laiendatud ohjemeetmeid. ISO/IEC 27018 järgi eraldiseisvat akrediteeritud sertifikaati ei ole. Ohjemeetmed võetakse ISO/IEC 27001 süsteemi rakendatavuse avaldusse ja sertifikaat väljastatakse seejärel standardi ISO/IEC 27001 järgi koos viitega standardile ISO/IEC 27018. Standard on suunatud avaliku pilveteenuse pakkujale, kes töötleb isikuandmeid oma pilveteenuse klientide nimel. Organisatsioon, kes pilveteenuseid üksnes kasutab, sellesse rolli ei astu ja hindab nõudeid mõistlikult oma pakkujate, mitte iseenda suhtes. Leanshifti jaoks on see kontrollnimekiri seetõttu eelkõige tarnijate hindamise raamistik. Iga punkti saab pakkujale küsimusena esitada ja GDPR artikli 28 kohase andmetöötluslepinguga kindlustada. Sellise hindamise tulemus on sisemine vastavuskirje või pakkuja hindamisprofiil, mitte sertifikaat. Nummerdamisest: peatükid A.2 kuni A.12 järgivad standardi lisas A toodud privaatsuse põhimõtteid ja punktid numbriga nagu A.11.6 on seal loetletud lisaohjemeetmed. Punktid numbriga nagu 8.10 või 5.34 viitavad ISO/IEC 27002:2022 ohjemeetmetele, mida standard pilve jaoks täpsustab. Punktid lisandiga (Grundsatz), mis tähendab põhimõtet, tulenevad peatüki enda põhimõttest, kui lisa A eraldi lisaohjemeetmed ei sisalda.

Ettevõtte	Kuupäev	Täitja
-----------	---------	--------

A.2 Nõusolek ja valikuvõimalus2

A.2.1Pilveteenuse pakkuja toetab pilveteenuse klienti andmesubjektide õiguste täitmisel, näiteks andmetega tutvumine, parandamine, kustutamine ja vastuväite esitamine. Vastutus ja tähtajad on lepingus määratud.

Dokument

Mille järgi seda näeb: Tõendiks on GDPR artikli 28 kohane andmetöötlusleping klausliga andmesubjektide õiguste täitmise toetamise kohta, koos teenuse enda tehniliste vahenditega: ekspordi-, parandamis- ja kustutamiskompleksid või dokumenteeritud tugikord koos reageerimistähtajaga. Küsimus tarnijale: millise funktsiooni või protsessi pakute, et saaksime andmetega tutvumise või kustutamise taotluse ühe kuu jooksul täita?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.2 (Grundsatz)Pilveteenuse klientide isikuandmeid töödeldakse üksnes kliendi dokumenteeritud juhiste alusel. Andmesubjektide nõusoleku hankimine jääb kliendi kui vastutava töötleja ülesandeks ja pakkuja sellest ette ei rutta.

Mille järgi seda näeb: Tõendiks on juhiste klausel andmetöötluslepingus ja tõend selle kohta, et pakkuja andmeid teisesel eesmärgil ei kasuta, näiteks teenuse privaatsusteade ja tootedokumentatsioon. Küsimus tarnijale: kas töötlete meie kliendiandmeid mingil viisil väljaspool meie juhiseid, näiteks toote parandamiseks või mudelite treenimiseks?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.3 Eesmärgi õiguspärasus ja määratlemine2

A.3.1Eesmärk, milleks pakkuja isikuandmeid töötleb, piirdub kokkulepitud teenuse osutamisega ja on lepingus nimetatud. Töötlemist pakkuja oma eesmärkidel ei toimu.

Dokument

Mille järgi seda näeb: Tõendiks on andmetöötlusleping, milles on esitatud töötlemise ees, laad, eesmärk ja kestus ning andmesubjektide kategooriad vastavalt GDPR artikli 28 lõikele 3. Küsimus tarnijale: palume lepingu lisa, mis kirjeldab töötlemise eesmärki ammendavalt. Väikesele ettevõttele piisab pakkuja standardsest andmetöötluse lisast, kui see sisaldab seda teavet.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.3.2

Pakkujale usaldatud isikuandmeid ei kasutata reklaamiks, turunduseks ega pakkuja muudel ärilistel eesmärkidel ilma eelneva sõnaselge nõusolekuta. Teenuse osutamine ei sõltu sellisest nõusolekust.

Mille järgi seda näeb: Tõendiks on sõnaselge lepingusäte, mis välistab ärilise teisese kasutuse, koos teenuse kasutustingimustega. Küsimus tarnijale: kinnitage kirjalikult, et kliendiandmeid ei kasutata reklaamiks, profiilialalüüsiks ega tehisintellekti (AI) mudelite treenimiseks. Kui see kinnitus puudub, ei sobi teenus isikuandmete jaoks.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.4 Kogumise piiramine

1

A.4 (Grundsisaks andmetele, mille klient teenusesse sisestab, pakkuja oma eesmärkidel täiendavaid isikuandmeid ei kogu, näiteks telemeetriat, kasutusprofiile ega sisuanalüüse. Kogutavad tegevusandmed ja metaandmed on nimetatud ja põhjendatud.

Mille järgi seda näeb: Tõendiks on loend andmetest, mida teenus sisuandmete kõrval salvestab (pääsulogid, telemeetria, diagnostikaandmed), koos eesmärgi ja säilitusajaga, ning ekraanitõmmis seadistusest, millega valikuline telemeetria välja lülitatakse. Küsimus tarnijale: milliseid kasutus-, telemeetria- ja diagnostikaandmeid kogute lisaks, milleks neid kasutate ja kas saame kogumise välja lülitada?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.5 Andmete minimeerimine

2

A.5.1

Isikuandmete töötlemisel tekkivad ajutised failid, näiteks ajutine salvestusruum, vahemälud või tagasivõtmise päevikud, kustutatakse turvaliselt kindlaksmääratud aja jooksul.

Mille järgi seda näeb: Tõendiks on töö- või kustutamiskord, milles on nimetatud ajutiste andmete säilitusaeg, mida toetab süsteemi konfiguratsioon, näiteks vahemälu eluiga (TTL) või ajastatud puhastustöö koos täitmislogiga. Küsimus tarnijale: millise aja järel kustutatakse vahemälud, ajutised failid ja vaheseisundid ning kuidas seda seiratakse?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

8.11

Kõikjal, kus käitamine, testimine või tugi reaalandmeid ei vaja, on isikuandmed maskeeritud, pseudonümiseeritud või anonümiseeritud. Töödeldavate andmete maht piirub sellega, mida teenus tegelikult vajab.

Mille järgi seda näeb: Tõendiks on reegel selle kohta, millised keskkonnad tohivad reaalandmeid näha, ning ekraanitõmmised või skriptid maskeerimisest, mida test- ja arendussüsteemides kasutatakse. Küsimus tarnijale: kas tugi- ja arendusmeeskonnad töötavad tootmisandmetega ja kui jah, siis milliste kaitsemeetmete all? Väikesele ettevõttele piisab reeglist, et testsüsteimid töötavad üksnes genereeritud näidisandmetega.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.6 Kasutamise, säilitamise ja avalikustamise piiramine

3

A.6.1

Kui pakkuja saab õiguslikult siduva nõude isikuandmete avaldamiseks, näiteks ametiasutuselt, teavitab ta pilveteenuse klienti eelnevalt niivõrd, kui võrd seadus seda lubab.

Mille järgi seda näeb: Tõendiks on lepinguline teavitamisklausel ja sisemine protsess ametiasutuste päringute jaoks koos nimetatud vastutajaga. Küsimus tarnijale: kas teavitate meid enne andmete üleandmist ja kas avaldate läbipaistvusaruande ametiasutuste päringute kohta? Ajakohane läbipaistvusaruanne on tugev tõend.

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.6.2

Kui pakkuja avaldab isikuandmeid kolmandatele isikutele, registreerib ta sündmuse jälgitaval kujul: kes andmed sai, millal see toimus, millised andmed olid hõlmatud ja millisele alusele avaldamine tugineb.

[Dokument](#)

Mille järgi seda näeb: Tõendiks on avalikustamiste register või tugipiletite ajalugu nende väljadega, isegi kui kandeid ei ole. Tühi, kuid ajakohasena hoitav register on vastuvõetav ja on väikesele ettevõttele praktiline tee. Küsimus tarnijale: kas peate andmete avaldamise registrit ja kas saame sellest väljavõtteid?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.10

Isikuandmed kustutatakse, kui kokkulepitud säilitusaeg lõpeb või leping lõpeb, sealhulgas varukoopiates olevad koopiad pärast nende rotatsioonitsükli.

Mille järgi seda näeb: Tõendiks on kustutamise kontseptsioon koos säilitusaegadega andmekategooriate kaupa, varukoopiate säilitusaeg ning kustutamislõgi või kustutamise kinnitus. Küsimus tarnijale: kui kaua meie andmed pärast lepingu lõppu varukoopiates püsivad ja kas saame nende kustutamise kohta kirjaliku kinnituse?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.7 Õigus ja kvaliteet

2

A.7 (Grund)

Pakkuja ei muuda talle usaldatud isikuandmeid omal algatusel. Parandused ja uuendused tehakse üksnes pilveteenuse kliendi juhisel või funktsioonide kaudu, mida klient ise kasutab.

Mille järgi seda näeb: Tõendiks on teenuse muutmisfunktsioonid koos muudatuste ajalooga ning juhiste klausel andmetöötuslepingus. Küsimus tarnijale: kas saame kirjeid ise parandada ja kas iga muudatus logitakse jälgitaval kujul?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

8.13

Isikuandmete terviklus on kaitstud salvestamisel, edastamisel ja taastamisel. Varukoopiad on olemas ja nende taastatavus on testitud.

Mille järgi seda näeb: Tõendiks on varukoopiate konfiguratsioon, kontrollsummad või terviklust tagavad mehhanismid ning vähemalt üks dokumenteeritud taastamise test aastas koos kuupäeva ja tulemusega. Küsimus tarnijale: kui sageli taastamist testite ja millise taasteaja teenustasemes tagate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8 Avatus, läbipaistvus ja teavitamine

2

A.8.1

Isikuandmeid töötlevate alltöötajate kasutamine avaldatakse enne lepingu sõlmimist. Loendi muudatustest teavitatakse klienti aegsasti, et klient saaks esitada vastuväite või lepingu lõpetada.

[Dokument](#)

Mille järgi seda näeb: Tõendiks on ajakohane alltöötajate loend, mis on avaldatud või lepinguga kättesaadavaks tehtud, koos nime, riigi ja töötlemise eesmärgiga, ning teavitamisreegel vastavalt GDPR artikli 28 lõikele 2. Küsimus tarnijale: kust leiame alltöötajate loendi, kui pika eettetamisaajaga muudatustest teatate ja kuidas saame vastuväite esitada?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.8 (Grund)

Enne lepingu sõlmimist teeb pakkuja kättesaadavaks arusaadava teabe selle kohta, kuidas isikuandmeid töödeldakse, millised kaitsemeetmed on olemas ja millistes õigusruumides töötlemine toimub.

Mille järgi seda näeb: Tõendiks on privaatsusteade, turbe ülevaatedokument, usalduskeskuse leht ja andmetöötusleping koos tehniliste ja korralduslike meetmetega lisana. Küsimus tarnijale: palume ajakohast tehniliste ja korralduslike meetmete loendit lepingu lisana, mitte üksnes turundusmaterjali.

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.9 Isiku kaasatus ja juurdepääs

2

A.9 (Grundsteen) Teenus annab pilveteenuse kliendile tehnilised vahendid, et andmesubjektide tutvumis-, parandamis- ja kustutamistaotlusi ise täita, näiteks ekspordi-, otsingu- ja kustutamiskutsioonide kaudu.

Mille järgi seda näeb: Tõendiks on ekspordi- ja kustutamismeeskonnade tootedokumentatsioon, mida toetab sisemine proovikäik: üks tutvumistaotlus tehakse algusest lõpuni läbi ja pannakse kirja, kui kaua see võtab. Küsimus tarnijale: kas saame ühe isiku kõik andmed leida, eksportida ja kustutada ilma teie toeta?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.34 Kui klient ei saa andmesubjekti taotlust ise täita, aitab pakkuja kokkulepitud aja jooksul. Taotlused, mille andmesubjektid saadavad otse pakkujale, edastatakse kliendile ja pakkuja neile ise ei vasta.

Mille järgi seda näeb: Tõendiks on vastav klausel andmetöötluslepingus koos konkreetse reageerimistähtajaga ning tugipiletite ajalugu tegeliku näitena. Küsimus tarnijale: millise tähtaia tagate andmesubjektide õiguste täitmise toetamisel ja mida see maksab?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.10 Aruandekohustus

4

A.10.1 Isikuandmetega seotud rikkumistest teatatakse pilveteenuse kliendile põhjendamatu viivitusega, nimetades ulatuse, mõjutatud andmed, põhjuse ja võetud meetmed. Teavitamisprotsess koos vastutuse ja tähtaegadega on määratletud.

Dokument

Millie järgi seda näeb: Tõendiks on juhtumile reageerimise plaan koos eskaleerimisahelaga, lepinguline teavitamistähtaeg (praktikas toimib 24 kuni 48 tundi, et klient jõuaks veel täita GDPR artiklis 33 sätestatud 72 tunni tähtaja) ning kirjed varasematest juhtumitest või õppusest. Küsimus tarnijale: millise aja jooksul juhtumist teatate, millise kanali kaudu ja millist teavet sellega edastate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.10.2 Infoturbepoliitikaid, töökordi ja nendega seotud kirjeid säilitatakse kindlaksmääratud aja, et töötlemise käiku saaks tagantiärele taastada.

Dokument

Mille järgi seda näeb: Tõendiks on säilitamisreegel koos poliitikate versioonijalalooga, näiteks dokumendiregistri või versioonihaldussüsteemi kaudu, milles on kinnitamise kuupäev. Küsimus tarnijale: kui kaua hoiate poliitikate versioone ja nendega seotud kirjeid ning kas saame auditi korral neile juurdepääsu?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.10.3 Isikuandmete tagastamiseks, üleandmiseks ja hävitamiseks lepingu lõppedes on olemas määratletud kord, milles on nimetatud vormingud, tähtajad ja koopiade käsitlemine.

Dokument

Mille järgi seda näeb: Tõendiks on lepingu lõpetamise klausel andmetöötluslepingus ning kustutamise kinnitus pärast lepingu lõppu. Küsimus tarnijale: millises vormingus ja millise aja jooksul saame oma andmed tagasi, millal hävitatakse kõik koopiad ja kas saame selle kohta kirjaliku kinnituse?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

5.35 Kaitsemeetmete tulemuslikkust vaadatakse sõltumatult üle kindlaksmääratud sagedusega, näiteks siseauditite, läbistustestide või kolmanda poole kinnitusaruannete kaudu. Tulemused tehakse pilveteenuse kliendile sobival kujul kättesaadavaks.

Millie järgi seda näeb: Tõendiks on ISO/IEC 27001 sertifikaat koos rakendatavuse avaldusega, mis hõlmab ISO/IEC 27018 ohjemeetmeid, või SOC 2 aruanne, koos ajakohaste läbistustestide kokkuvõtetega. Küsimus tarnijale: palume sertifikaati, selle käsitlusala ja kinnitust, et ISO/IEC 27018 kajastub rakendatavuse avalduses. Kontrollimist väärib, kas käsitlusala hõlmab tegelikult kasutatavat teenust.

	Ayatud	Töös	Täidetud	Ei kohaldu
--	--------	------	----------	------------

Tõend / põhjendus

A.11 Infoturvet

13

A.11.1

Kõik, kellel on juurdepääs isikuandmetele, on seotud konfidentsiaalsuskohustusega, olenemata sellest, kas nad on otse tööle võetud või väljastpoolt kaasatud.

Mille järgi seda näeb: Tõendiks on allkirjastatud konfidentsiaalsuslepingud või kohustused, mis kehtivad ka pärast koostöö lõppu. Küsimus tarnijale: kas kõik andmetele juurdepääsu omavad töötajad ja teenusepakkujad on kirjalikult konfidentsiaalsuskohustusega seotud?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.2

Isikuandmeid sisaldavaid väljatrükke ja muid paberkoopiaid tehakse üksnes hädavajaduse korral. Lubatud ulatus on reeglina määratud.

Mille järgi seda näeb: Tõendiks on väljatrükkide käsitlemise reegel, mis andmekeskustes tähendab tavaliselt üldist printimise keeldu aladel, kus hoitakse kliendiandmeid. Küsimus tarnijale: kas kliendiandmeid teie tegevuses üldse prinditakse ja kui jah, siis millistel tingimustel?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.3

Varukoopiatest taastamine kiidetakse eelnevalt heaks ja logitakse, sealhulgas taastamise käivitunud isik ja mõjutatud andmed.

Mille järgi seda näeb: Tõendiks on taastamislogi koos ajatempli, algataja ja ulatusega, mille varunduse tööriist tavaliselt automaatselt loob. Küsimus tarnijale: kas logite iga taastamise ja kas saame auditi korral neid logisid vaadata?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.4

Isikuandmeid sisaldavad andmekandjad, mis viiakse tegevuskohast välja, on kaitstud volitamata pääsu ja kaotsimineku eest, üldjuhul krüpteerimise ja transpordikirje abil.

Mille järgi seda näeb: Tõendiks on krüpteerimise tõend (andmekandja täielik krüpteerimine), transpordi- ja üleandmiskirjed ning andmekandjate register. Küsimus tarnijale: kas kliendiandmeid sisaldavad andmekandjad lahkuvad kunagi teie asukohtadest, näiteks varukoopiade jaoks, ja kuidas need on teel kaitstud?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.5

Krüpteerimata kaasaskantavate andmekandjate ja seadmete kasutamine isikuandmete jaoks on keelatud või piiratud põhjendatud eranditega, millel on dokumenteeritud heakskiit.

Mille järgi seda näeb: Tõendiks on irdkandjate poliitika ning tehniline jõustamine, näiteks kohustuslik seadme krüpteerimine või seadmehalduse kaudu blokeeritud USB-pordid. Küsimus tarnijale: kas töötajad saavad kliendiandmeid krüpteerimata seadmetele kopeerida ja mis seda tehniliselt takistab?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.6

Avalike võrkude kaudu edastatavad isikuandmed on krüpteeritud. Kasutatavad mehhanismid vastavad praegusele tehnika tasemele.

Mille järgi seda näeb: Tõendiks on TLS-i konfiguratsioon (ajakohane protokolliversioon, vananenud šifreid ei ole) ja väline konfiguratsioonitest aruandena. Väikesele ettevõttele on praktiline teha kord aastas tasuta TLS-i skannimine ja tulemus talletada. Küsimus tarnijale: millise transpordikrüpteerimise jõustate ja kas salvestatud andmete krüpteerimine on aktiivne?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.7

Isikuandmeid sisaldavad paberkirjed hävitatakse viisil, mis välistab nende taastamise.

Mille järgi seda näeb: Tõendiks on piisava turvasemega dokumendihävitid või hävitamistõendid teenusepakkujalt, kes töötab standardi DIN 66399 või samaväärse standardi järgi. Küsimus tarnijale: kuidas hävitatakse klientidega seotud paberkirjed ja kas hävitamistõendid on talletatud?

Avatud

Töös

Täidetud

Ei kohaldu

Tõend / põhjendus

A.11.8 Kasutajatunnused on omistatud üheselt ühele isikule ning neid ei anta uuesti välja ega jagata. Jagatud kontod on olemas üksnes põhjendatud eranditena ja täiendava jälgitavusega.

Mille järgi seda näeb: Tõendiks on identiteedisüsteemist pärit kasutajate loend, milles rühmakontosid ei ole, koos reegluga, et haldustööd tehakse isikliku konto alt. Küsimus tarnijale: kas teie halduspersonal töötab isiklike kontodega ja kas mitmeastmeline autentimine on kohustuslik?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.11.9 Pakkuja saab igal ajal öelda, millised isikud või rollid tohivad isikuandmetele juurde pääseda, ja hoiab selle ülevaate ajakohasena.[Dokument](#)

Mille järgi seda näeb: Tõendiks on pääsuõiguste ülevaade rollide kaupa, mida toetab korduv pääsuõiguste ülevaatus koos kuupäeva ja tulemusega. Väikesele ettevõttele piisab kasutajate loendi poolaastasest väljavõttest koos kinnitusega. Küsimus tarnijale: kui paljud teie töötajad pääsevad meie andmetele ligi ja kui sageli seda üle vaatate?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.11.10 Kasutajakontosid hallatakse kogu olelusringi ulatuses: loomine, muutmine ja kiire deaktiveerimine, kui keegi lahkub või rolli vahetab.

Mille järgi seda näeb: Tõendiks on tööle võtmise ja töölt lahkumise kord koos kontrollnimekirjaga ning deaktiveeritud kontode logid koos ajatemplitega. Küsimus tarnijale: millise aja jooksul võtate lahkuvatelt töötajatelt pääsuõigused ära ja kuidas seda tõendate?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.11.11 Pakkuja turbe- ja privaatsuskohustused on lepingus kindlaks määratud, sealhulgas tehnilised ja korralduslikud meetmed, kliendi juhiste siduvus ning kliendi õigus auditeerida.[Dokument](#)

Mille järgi seda näeb: Tõendiks on allkirjastatud GDPR artikli 28 kohane andmetöötlusleping koos meetmete lisaga ning auditi- või teabeõigusega. Küsimus tarnijale: palume allkirjastatud andmetöötluslepingut koos lisadega, mitte üksnes viidet üldistele kasutustingimustele.

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.11.12 Isikuandmeid töötlevatele alltöötlejatele kehtivad vähemalt samad kohustused mis pakkuja endale. Nende valikut ja jooksvat seiret reguleerib määratletud protsess.

Mille järgi seda näeb: Tõendiks on kohustuste edasiandmine alltöötlejatega sõlmitud lepingutes (GDPR artikli 28 lõige 4) ja kuupäeva kandev tarnija hindamine. Küsimus tarnijale: kuidas hindate oma alltöötlejaid ja milliseid tõendeid neilt nõuate?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.11.13 Enne salvestusruumi taaskasutamist on tagatud, et varasemate kasutajate andmed ei jää kättesaadavaks, ei füüsilistel andmekandjatel ega virtualiseeritud keskkondades.

Mille järgi seda näeb: Tõendiks on puhastamise või ülekirjutamise kord, mida kohaldatakse salvestusruumi vabastamisel, andmekandjate hävitamise kirjed ning arhitektuuridokumendis kirjeldatud klientide eraldatus. Küsimus tarnijale: kuidas tagate, et taaskasutatavas salvestusruumis ei ole teiste klientide jääkandmeid?

Avatud Töös Täidetud Ei kohaldu

Tõend / põhjendus

A.12 Privaatsusnõuetele vastavus

3

A.12.1 Riigid, kus isikuandmeid säilitatakse ja töödeldakse, on nimetatud ja pilveteenuse kliendile teada. Salvestuskohtade muudatustest teavitatakse.[Dokument](#)

Mille järgi seda näeb: Tõendiks on pakkuja ülevaade asukohtadest ja piirkondadest, kas lepingus või dokumentatsioonis, ning ekraanitõmmis kasutatava teenuse piirkonnaseadistusest. Küsimus tarnijale: millistes riikides meie andmed salvestatuna asuvad, millistest riikidest neile ligi pääsetakse, näiteks toe käigus, ja kas saame piirkonna fikseerida?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

A.12.2 Isikuandmete edastamine kolmandatesse riikidesse on teada, põhjendatud ja kaetud asjakohaste kaitsemeetmetega.[Dokument](#)

Mille järgi seda näeb: Tõendiks on lepingu tüüptingimused või kaitse piisavuse otsus, mida toetab edastuse mõjuhindang, mis väikeses ettevõttes võib olla lühike: hõlmatud andmekategooriad, sihtriik, risk, võetud lisameetmed. Küsimus tarnijale: millisel õiguslikul alusel edastate andmeid kolmandatesse riikidesse ja milliseid täiendavaid meetmeid kohaldate?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus

5.31 Isikuandmete töötlemisele kohalduvad õiguslikud ja lepingulised nõuded on tuvastatud ning neid hoitakse õigusliku olukorra muutudes ajakohasena. Vastuolulised õigusruumid on hinnatud.

Mille järgi seda näeb: Tõendiks on kohalduvate nõuete ülevaade (GDPR, riigisisesed reeglid, valdkonnapõhised kohustused) koos vastutaja ja ülevaatuse kuupäevaga. Väikeses ettevõttes piisab ühelehelisest loendist, mis vaadatakse üle kord aastas. Küsimus tarnijale: kas teie või teie alltöötajad alluvad õigusruumidele, mis lubavad ametiasutustel meie andmetele ligi pääseda, ja kuidas sellega toime tulete?

Avatud	Töös	Täidetud	Ei kohaldu
--------	------	----------	------------

Tõend / põhjendus