					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P33S					Dokumendi pealkiri: **Auditi ja vastavusseire poliitika**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 9.2, 10	Siseauditid, pidev täiustamine ja mittevastavuste parandusmeetmed
ISO/IEC 27002:2022	Kontrollid 5.35, 5.37	Kavandatud sisemised läbivaatamised, sõltumatud ülevaatused sisseostetud protsesside puhul
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Turvahindamised, vastavuse pidev seire, auditite läbivaatamine/analüüs ja aruandlus
GDPR	Artiklid 24 ja 32	Tehniliste ja korralduslike meetmete auditeerimine, tõendid kontrollimeetmete tõhususe kohta
NIS2	Artikkel 21(2)(f)	Ennetav läbivaatamine ja tõenduspõhine vastavus
DORA	Artikkel 10	IKT-riski juhtimine, seire ja aruandlus
COBIT 2019	MEA01, MEA03	Seire ja vastavuse hindamine, valmisolek kolmandate osapoolte läbivaatamisteks

1. Eesmärk

1.1 Käesolev poliitika sätestab organisatsiooni lähenemise siseauditite, turbekontrollide ja õigusnõuetele vastavuse seire läbiviimisele. See tagab, et kõik kontrollimeetmed, poliitikad, süsteemid ja teenuseosutajad vaadatakse korrapäraselt ning struktureeritult läbi.

1.2 Eesmärk on tuvastada kontrollimeetmete rikked, ennetada mittevastavust ja tõendada hoolsuskohustuse täitmist ISO/IEC 27001, GDPR-i ja seotud raamistikest tulenevate nõuete alusel.

1.3 See võimaldab VKE-del säilitada tegevusliku kontrolli ja valmisoleku sertifitseerimiseks ka ilma eraldi vastavusfunktsioonita, kasutades lihtsaid, korratavaid kontrollnimekirju ja riskipõhiselt prioriseeritud auditileide.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõik sisemised üksused ja välised teenuseosutajad, kellel on vastutus IT-süsteemide, isikuandmete ja ärikriitiliste teenustega seotud tegevuste eest;

2.1.2 kõik kontrollimeetmed ja süsteemid, mis kuuluvad infoturbe juhtimissüsteemi (ISMS) kohaldamisalasse;

2.1.3 kõik siseauditid, turbekontrollide ülevaatused ja vastavuskontrollid, sõltumata sellest, kas neid teeb organisatsioon ise või väline konsultant, klient või reguleeriv asutus.

2.2 Käesolev poliitika kohaldub ka tõendusmaterjali kogumisele ja aruandlusele järgmistel eesmärkidel:

2.2.1 ISO/IEC 27001 sertifitseerimis- ja taasertifitseerimisauditid;

2.2.2 andmekaitseauditid GDPR-i või lepingutingimuste alusel;

2.2.3 klientide algatatud turbeküsimustikud või hoolsusauditi läbivaatamised;

2.2.4 kõik NIS2 või DORA alusel tehtavad regulatiivsed või sõltumatud läbivaatamised, kui need on asjakohased.

3. Eesmärgid

3.1 Tagada, et kõik peamised kontrollimeetmed ja poliitikad vaadatakse korrapäraselt läbi nende tõhususe ja vastavuse hindamiseks.

3.2 Säilitada auditijälg ja parandusmeetmete kirjed, et tõendada vastutust ja pidevat täiustamist.

3.3 Valmistuda sertifitseerimiseks, taasertifitseerimiseks ja kliendikindluse programmideks (nt ISO 27001, tarnija kaasamise protsess).

3.4 Tuvastada puudujäägid varakult, et võimaldada kiiret kõrvaldamist enne probleemide eskaleerumist või nõuete rikkumist.

3.5 Võimaldada tegevjuhil ja IT-teenuse osutajal koordineerida läbivaatamisi minimaalse keerukusega, tagades samal ajal kaitstavad tulemused.

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 teeb järelevalvet auditiprogrammi üle;

4.1.2 kiidab heaks sisemised läbivaatamiskavad ja auditileiud;

4.1.3 määrab parandusmeetmed ja jälgib nende täitmist;

4.1.4 annab loa väliste audiitorite või konsultantide kaasamiseks.

4.2 IT-toe teenuseosutaja / sisemine IT-vastutaja

4.2.1 esitab sise- ja välisauditite käigus tõendusmaterjali (nt logid, konfiguratsioonid, juurdepääsukontrolli kirjed);

4.2.2 toetab tehniliste kontrollide ülevaatust (nt varunduse olek, paikade rakendamise vastavus);

4.2.3 haldab auditi tõendusmaterjali hoidlat.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Poliitika ja auditiplaani iga-aastane läbivaatamine

9.1.1 Tegevjuht (GM) peab käesoleva poliitika ja auditi ajakava läbi vaatama vähemalt üks kord aastas.

9.1.2 Läbivaatamisel tuleb hinnata järgmist:

9.1.2.1 auditite tulemuslikkus puudujääkide tuvastamisel;

9.1.2.2 auditite ja parandusmeetmete lõpuleviimise määr;

9.1.2.3 kohaldatavate õiguslike, regulatiivsete või sertifitseerimisnõuete muudatused.

9.2 Sündmuspõhised ajakohastamised

9.2.1 Poliitika tuleb läbi vaadata ja ajakohastada, kui:

9.2.2 sertifitseerimis- või järelevalveaudit tuvastab olulise mittevastavuse;

9.2.3 õiguslikud või regulatiivsed raamistikud muutuvad (nt uus GDPR-i suunis, NIS2 riigisisene rakendamine);

9.2.4 ärimuudatused mõjutavad süsteeme, protsesse või tarnijaid, mis kuuluvad auditi kohaldamisalasse;

9.2.5 kriitiline intsident või rikkumine toob esile varem tuvastamata kontrollimeetmete puudujäägid.

9.3 Muudatuste dokumenteerimine

9.3.1 Kõiki muudatusi tuleb jälgida poliitika versioonihalduse logis.

9.3.2 Ajakohastused tuleb edastada kõigile auditite ga seotud meeskonnaliikmetele.

9.3.3 Uuendatud poliitikale tuleb lisada muudatuste kokkuvõte, et tagada ühtne arusaam.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat toetavad ja täiendavad mitmed teised VKE poliitikad:

10.1.1 P1S – Infoturbepoliitika: määrab kõigi kontrollimeetmete ootuste baastaseme ja nõuab nende järgimise kontrollimist auditite kaudu.

10.1.2 P2S – Juhtimisrollide ja vastutuste poliitika: kehtestab vastutuse auditi kavandamise, läbiviimise ja parandusmeetmete eest.

10.1.3 P6S – Riskijuhtimise poliitika: tuvastab auditites ilmnenud kontrollimeetmete nõrkused ja tagab auditileidude dokumenteerimise riskiregistris.

10.1.4 P17S – Andmekaitse ja privaatsuspoliitika: määratleb GDPR-i kontrollimeetmed, mida tuleb auditeerida, sealhulgas andmete töötlemine, rikkumistele reageerimine ja andmekaitseteadete haldamine.

10.1.5 P22S – Logimis- ja seirepoliitika: tagab vastavus- ja kontrollimeetmete ülevaatuste käigus kasutatavad auditilogid ja kohtueksperti isi andmed.

10.1.6 P30S – Intsidentidele reageerimise poliitika: nõuab intsidendikirjete ja intsidendijärgsete ülevaatuste perioodilist auditeerimist, et verifitseerida reageerimise tõhusust.

10.1.7 P31S – Tõendusmaterjali kogumise ja kohtueksperti isi poliitika: sätestab protseduurid auditite käigus verifitseeritava tõendusmaterjali kogumiseks ja tõendite valduse ahela säilitamiseks.

10.2 Koos loovad need poliitikad suletud tsükliga kontrollikeskkonna, mis võimaldab sisemist verifitseerimist, välist kindlust ja standarditega kooskõlas olevat juhtimist.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001:

11.1.1 Punkt 9.2 – nõuab siseauditite läbiviimist, et hinnata ISMS-i toimivust ja vastavust nõuetele.

11.1.2 Punkt 10.1 – nõuab pidevat täiustamist auditi tulemuste ja mittevastavuste parandusmeetmete alusel.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 5.35 – nõuab kontrollimeetmete ja protsesside kavandatud sisemisi läbivaatamisi.

11.2.2 Kontroll 5.37 – rõhutab sõltumatute ülevaatuste vajadust, eelkõige sisseostetud protsesside puhul.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – turvahindamised: nõuab rakendatud kontrollimeetmete auditeerimist nende tõhususe verifitseerimiseks.

11.3.2 CA-7 – vastavuse pidev seire: rõhutab kontrollimeetmete nõrkuste ennetavat tuvastamist ja läbivaatamist.

11.3.3 AU-6 – auditite läbivaatamine, analüüs ja aruandlus: nõuab auditilogide ja auditileidude korrapärast analüüsi ning käsitlemist.

11.4 GDPR:

11.4.1 Artiklid 24 ja 32 – nõuavad tehniliste ja korralduslike meetmete rakendamist ja auditeerimist, sealhulgas tõendeid kontrollimeetmete tõhususe ja ajas toimuva täiustamise kohta.

11.5 NIS2 direktiiv (EL) 2022/2555:

11.5.1 Artiklid 20–21 – nõuavad ennetavat kontrollimeetmete läbivaatamist, tõenduspõhist vastavust ja auditeeritavust oluliste ja tähtsate üksuste puhul.

11.6 COBIT 2019:

11.6.1 MEA01 – tulemuslikkuse ja vastavuse seire, hindamine ja auditeerimine: nõuab protsesside ja kontrollimeetmete toimivuse perioodilist hindamist standardite ja eesmärkide suhtes.

11.6.2 MEA03 – välisnõuetele vastavuse tagamine: keskendub sisemisele seirele ja valmisolekule kolmandate osapoolte audititeks ning regulatiivseteks läbivaatamisteks.