					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P12S					Dokumendi pealkiri: **Varahalduse 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 õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	varahalduse nõuded
ISO/IEC 27002:2022	Kontroll 5	varahalduse kontrollimeetmed
NIST SP 800-53 Rev.5	CM-8	süsteemikomponentide register
EL NIS2	Artikkel 21(2)(a)	varade jälgimine võrgu- ja infosüsteemide kaitseks
EL DORA	Artikkel 5(8)	IKT-varade registri nõuded
COBIT 2019	BAI	IT-varade olelusringi haldus
EL GDPR	Artikkel 30	isikuandmete töötlemistoimingute register

1. Eesmärk

1.1 Käesolev poliitika määratleb, kuidas organisatsioon tuvastab, jälgib, kaitseb ja kõrvaldab kasutuselt oma teabevarasid, sealhulgas nii füüsilisi kui ka digitaalseid komponente.

1.2 Eesmärk on vähendada tegevus- ja turberiske, tagades kõigi ärivarade nähtavuse, vastutuse ja turvalise käitlemise kogu nende olelusringi vältel.

1.3 Usaldusväärne varade register toetab õigusaktidele vastavust, intsidentidele reageerimist, talitluspidevuse planeerimist ja riskijuhtimist.

1.4 Käesolev poliitika toetab ka sertifitseerimist standardi ISO/IEC 27001 alusel ning tõendab kooskõla GDPR-ist, NIS2-st ja DORA-st tulenevate õiguslike, finants- ja küberturbealaste kohustustega.

1.5 Väikeste ja keskmise suurusega ettevõtete (VKE-de) jaoks on lihtne, kuid süsteemne varahalduse käsitlus hädavajalik, et vältida haldamata seadmeid, andmekadu või auditi ebaõnnestumist, eriti piiratud tehnilise personali tingimustes.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile varadele, mis kuuluvad organisatsioonile, on renditud või mida organisatsioon muul viisil haldab, sealhulgas varadele, mida kasutatakse järgmistes keskkondades:

2.1.1 kontoripõhine töö

2.1.2 kaug- või hübriidtöö

2.1.3 välitöö või mobiilsed tegevused

2.1.4 pilve- ja allhankekeskkonnad

2.2 Hõlmatud varaliigid hõlmavad muu hulgas järgmist:

2.2.1 riistvara: sülearvutid, lauaarvutid, monitorid, telefonid, tahvelarvutid, USB-mäluseadmed, ruuterid, printerid, varunduskandjad

2.2.2 tarkvara: paigaldatud rakendused, SaaS-tööriistad, operatsioonisüsteemid, viirusetõrjevahendid, litsentsid

2.2.3 andmevarad: äriandmete hoidlad, arvutustabelid, kliendikirjed, lähtekood

2.2.4 digitaalsed autentimisandmed ja teenused: domeeninimed, digitaalsed sertifikaadid, API-võtmed, e-posti kontod, pilveteenuste sisselogimisandmed

2.2.5 juurdepääsuvahendid: võtmed, kiipkaardid, juurdepääsupuldid, biomeetrilised tõendid

2.3 Käesoleva poliitika kohaldamisalasse kuuluvad kõik töötajad, töövõtjad ja kolmandatest osapooltest teenuseosutajad, kes käitlevad organisatsiooni varasid.

2.4 Poliitika reguleerib nii lühiajalisi varasid (nt projektipõhised sülearvutid) kui ka pikaajalisi varasid, samuti mitme töötaja poolt kasutatavaid ühiskasutatavaid varasid.

3. Eesmärgid

3.1 Kehtestada ja hallata täielik ning täpne kõigi asjakohaste varade register, mida ajakohastatakse pidevalt.

3.2 Tagada, et igale varale on määratud varaomanik, kes vastutab selle kasutamise, hoiustamise ja tagastamise eest.

3.3 Klassifitseerida varad tundlikkuse, ärimõju või regulatiivse asjakohasuse alusel, võimaldades rakendada diferentseeritud kaitsetasemeid.

3.4 Määratleda selged protseduurid vara väljastamiseks, ümbermääramiseks, hoolduseks, kadumisest teatamiseks ja kasutuselt kõrvaldamiseks.

3.5 Tagada varade turvaline käitlemine kogu nende olelusringi vältel ning see, et nendele salvestatud teave oleks kasutuselt kõrvaldamisel kas kaitstud või turvaliselt kustutatud.

3.6 Vähendada selliste turbeintsidentide tõenäosust, mis on põhjustatud jälgimata, tagastamata või väärkasutatud organisatsiooni ressurssidest.

3.7 Toetada asjakohaste õigusaktide (nt GDPR-i vastutuse põhimõtte) ning küberturbe sertifitseerimisstandardite nõuetele vastavust.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Vastutab käesoleva poliitika eest ning tagab, et varahalduse tavasid rakendatakse ja järgitakse kogu organisatsioonis.

4.1.2 Vaatab läbi ja kinnitab varade registri ajakohastused ning annab vajaduse korral loa vara kasutuselt kõrvaldamiseks või üleandmiseks.

4.1.3 Teda tuleb teavitada igast olulisest vara kaotusest, vargusest või väärkasutusest.

4.2 IT-juht või määratud varahaldur

4.2.1 Haldab varade registrit (nt arvutustabelis, piletisüsteemis või lihtsustatud varahalduslahenduses).

4.2.2 Määrab varaomanikud ja jälgib staatuse muudatusi (nt uus, kasutuses, remondis, kasutuselt kõrvaldatud).

4.2.3 Kontrollib, et kõik väljastatud varad on dokumenteeritud ja seotud konkreetse isiku või äriüksusega.

4.2.4 Tagab, et klassifitseerimismärgised on rakendatud ja neid järgitakse (nt sisekasutuseks, konfidentsiaalne).

4.2.5 Koordineerib varade tagasivõtmist, puhastamist ja deaktiveerimist töösuhte lõpetamise protsessi või kasutuselt kõrvaldamise käigus.

4.2.6 Teatab lahendamata varade lahknevustest tegevjuhile.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt üks kord aastas ja alati, kui:

9.1.1 võetakse kasutusele uut tüüpi tehnoloogiaid või varasid

9.1.2 vara jälgimise protseduurid muutuvad (nt uute tööriistade või platvormide kasutuselevõtul)

9.1.3 uued regulatiivsed kohustused mõjutavad varade jälgitavust või kõrvaldamist

9.1.4 intsident või audit tuvastab puudujäägi kehtivates varahalduse tavades

9.2 Läbivaatamisse tuleb kaasata tegevjuht ja IT-juht ning see peab hõlmama vara käitlemise protseduuride, registri mallide ja klassifitseerimissuuniste ajakohastamist.

9.3 Kõik ajakohastused tuleb dokumenteerida ja asjassepuutuvale personalile teatavaks teha. Säilitada tuleb versioonihaldusega muudatuste logi.

10. Seotud poliitikad ja seosed

10.1 P2S – Juhtimisrollide ja vastutuste poliitika: määrab vastutuse poliitika omaniku rolli ja IT-tegevuste eest.

10.2 P4S – Juurdepääsukontrolli poliitika: seob vara kasutamise (nt sülearvutid, mobiilsed seadmed) kasutajate juurdepääsuõiguste ja identiteedihalduse protsessidega.

10.3 P7S – Töölevõtu ja töösuhte lõpetamise poliitika: tagab, et vara väljastamine ja tagastamine on personali olelusringi protsessidesse sisse ehitatud.

10.4 P13S – Andmete klassifitseerimise ja märgistamise poliitika: sätestab reeglid, mille alusel määrata, kas vara tuleb klassifitseerida sisekasutuseks või konfidentsiaalseks.

10.5 P30S – Intsidentidele reageerimise poliitika: reguleerib reageerimisprotseduure juhul, kui varaga seotud sündmus põhjustab turbe- või andmekaitserikkumise.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1: nõuab operatiivseid kontrollimeetmeid varade haldamiseks ja nende kaitsmiseks kogu kasutusaja vältel.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.9: kirjeldab, kuidas varasid tuvastada, määrata neile omanik, klassifitseerida ja turvaliselt hallata.

11.3 NIST SP 800-53 Rev.5

11.3.1 CM-8: nõuab organisatsioonidelt süsteemikomponentide registri loomist ja haldamist, sealhulgas riistvara, tarkvara ja virtuaalvarade kohta.

11.4 EL GDPR

11.4.1 Artikkel 30: nõuab isikuandmete töötlemistoimingute dokumenteerimist, mis eeldab teadmist, kus andmeid hoitakse ja millistel varadel.

11.5 EL NIS2

11.5.1 Artikkel 21(2)(a): nõuab tehnilisi ja korralduslikke meetmeid, sealhulgas varade jälgimist, võrgu- ja infosüsteemide kaitseks.

11.6 EL DORA

11.6.1 Artikkel 5(8): finantssektori üksused peavad IKT-riskide juhtimise osana haldama üksikasjalikke IKT-varade registreid.

11.7 COBIT 2019

11.7.1 BAI09: sätestab, et IT-varasid tuleb hallata kogu nende olelusringi vältel alates soetamisest kuni kasutuselt kõrvaldamiseni koos selge omandivastutuse ja kontrollimeetmetega.