					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P03					Dokumendi pealkiri: **IT-vahendite lubatud kasutuse 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**

Kohaldatavad standardid ja õigusnormid

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 5	Kehtestab AUP jaoks käitumisreeglid ja nõuded
ISO/IEC 27002:2022	Kontrollimeetmed 6.1, 6.2, 8.1, 8.12	Annab suunised infoturbealaste vastutuste, teadlikkuse ning seadmete ja andmete halduse kohta
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	IT-varade kasutamisega seotud juurdepääsukontrolli ning teadlikkuse ja käitumise kontrollid
ELi GDPR	Artiklid 5(1)(f), 32; põhjendus 39	Nõuab konfidentsiaalsuse ja tervikluse tagamist, tehniliste ja korralduslike meetmete rakendamist ning andmete nõuetekohase kasutamise õigusliku aluse olemasolu
ELi NIS2	Artikkel 21(2)(a–d)	Nõuab operatiivpoliitikaid ja turvalise kasutamise alast koolitust
ELi DORA	Artikkel 5	Toetab IKT-riskijuhtimist, reguleerides kasutajate käitumist
COBIT 2019	APO07, BAI05, DSS05, MEA01	Personalijuhtimine, muudatuste juhtimine, hallatud turve ning vastavuse ja tulemuslikkuse seire

1. Eesmärk

1.1 Käesolev poliitika määratleb organisatsiooni infosüsteemide, IT-vahendite, sidevahendite ja andmete lubatud ning lubamatu kasutuse.

1.2 Sellega tagatakse, et kõik kasutajad mõistavad oma vastutust ettevõtte IT-varade kasutamisel ning et nende tegevus toetab teabe konfidentsiaalsust, terviklust, käideldavust ja õiguspärast töötlemist.

1.3 Poliitika täidab ISO/IEC 27001:2022 punkti 5.10 nõudeid, kehtestades süsteemide kasutamise käitumisreeglid ning rakendades tehnilisi ja menetluslikke kontrollimeetmeid, et vähendada väärkasutuse, hooletuse või kuritarvituse riski.

1.4 Poliitika toetab ka uurimis- ja rakendustegevusi, sealhulgas intsidendikäsitlust ja rikkumiste korral kohaldatavaid distsiplinaarmeetmeid.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile isikutele ja üksustele, kellele on antud juurdepääs organisatsiooni infosüsteemidele ja varadele, sealhulgas, kuid mitte ainult:

2.1.1 töötajatele, töövõtjatele, konsultantidele, praktikantidele ja renditöötajatele;

2.1.2 kolmandatest osapooltest tarnijatele, kellel on süsteemijuurdepääs või delegeeritud haldusõigused;

2.1.3 külalistele või partneritele, kes kasutavad organisatsioonile kuuluvaid või organisatsiooni poolt lubatud IT-taristuid.

2.2 Kohaldamisala hõlmab kõiki organisatsiooni tehnoloogia- ja andmevarasid, sealhulgas:

2.2.1 tööjaamu, sülearvuteid, mobiilseadmeid ja servereid;

2.2.2 võrgutaristut ja pilvekeskkonnas majutatud teenuseid;

2.2.3 e-posti, sõnumsidevahendeid, failisalvestust, koostööplatvorme ja VPN-ühendusi;

2.2.4 puhkeolekus, edastamisel või töötlemisel olevaid andmeid, olenemata nende vormingust või asukohast;

2.2.5 isiklikke seadmeid, mida kasutatakse BYOD-i (oma seadme kasutamine töös) korra alusel ja mis ühenduvad organisatsiooni süsteemidega.

2.3 Käesolev poliitika kehtib kõigis töökeskkondades, sealhulgas:

2.3.1 ettevõtte kontorites ja tootmisüksustes;

2.3.2 kaugtöö asukohtades või hübriidtöö korralduse puhul;

2.3.3 välitöödel või kolmanda osapoole hallatavates ruumides.

2.4 Kõik kasutajad peavad kinnitama, et nad on käesolevast poliitikast teadlikud, ning järgima seda ettevõtte süsteemidele juurdepääsu või ettevõtte andmete töötlemise eeltingimusena.

3. Eesmärgid

3.1 Määratleda ja rakendada organisatsiooni IT-vahendite lubatud kasutuse reeglid.

3.2 Ennetada loata juurdepääsu, andmeleket või kahju, mis tuleneb hooletust või pahatahtlikust kasutusest.

3.3 Kaitsta ettevõtte võrke, varasid ja andmeid ohtude eest, mis tulenevad kasutajate käitumisest.

3.4 Toetada õiguslike ja lepinguliste kohustuste täitmist, tõendades nõuetekohast hoolsust IT-vahendite haldamisel.

3.5 Tagada distsiplinaarmeetmete ja erandite haldamise protsesside järjepidev ja selge rakendamine.

3.6 Edendada digitaalsete ja füüsiliste IT-vahendite eetilise, turvalise ja vastutustundliku kasutamise kultuuri.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kinnitab lubatud kasutuse poliitika (AUP) ning tagab selle kooskõla ärieesmärkide, regulatiivsete nõuete ja organisatsiooni väärtustega.

4.1.2 Eraldab ressursid poliitika rakendamiseks, koolituseks, seireks ja läbivaatamiseks.

4.1.3 Vaatab ISMS-i juhtimise osana läbi vastavuse seisu ja poliitika rikkumistega seotud distsiplinaarmeetmed.

4.2 IT- ja infoturbemeeskonnad

4.2.1 Rakendavad käesoleva poliitika jõustamiseks tehnilisi kontrollimeetmeid, sealhulgas:

4.2.2 sisufiltreerimist, pahavarakaitset, lõppseadmete turvet ja võrgu seire tööriistu;

4.2.3 e-posti turbekonfiguratsioone ja andmekao vältimise (DLP) lahendusi;

4.2.4 keelatud ja lubatud tarkvara, riistvara ning veebisaitide loendeid;

4.2.5 peavad arvestust heakskiidetud ja keelatud tarkvara, seadmete ning teenuste üle;

4.2.6 uurivad kahtlustatavaid AUP rikkumisi, koguvad digitaalseks kohtueksperti isiks sobivat tõendusmaterjali ning toetavad asjakohasel juhul distsiplinaar- või õiguslike meetmete rakendamist;

4.2.7 teevad personali- ja õigusfunktsiooniga koostööd intsidendikäsitluse, eskaleerimise ja teavitamiskohustuste täitmisel.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Läbivaatamise alused ja sagedus

9.1.1 Käesolev poliitika tuleb läbi vaadata:

9.1.1.1 vähemalt üks kord aastas;

9.1.1.2 pärast olulisi tehnoloogia- või taristumuudatusi;

9.1.1.3 pärast intsidente või auditileide, mis toovad esile rakendamise puudujäägid;

9.1.1.4 vastusena kohaldatavates õigusnormides või lepingutes tehtud muudatustele.

9.2 Omanik ja kinnitamine

9.2.1 Läbivaatamisprotsessi eest vastutab CISO või määratud ISMS-i juht.

9.2.2 Muudatused peab kinnitama tippjuhtkond ning neist tuleb teavitada kogu organisatsiooni.

9.2.3 Ajakohastatud tingimuste kinnitus tuleb poliitika uuesti väljastamisel uuesti koguda.

9.3 Dokumendihaldus

9.3.1 Poliitika peab sisaldama järgmist metaandmestikku ja versioonihalduse teavet:

9.3.1.1 pealkiri, tunnus ja klassifikatsioonitase;

9.3.1.2 poliitika omanik ja dokumendi eest vastutav haldur;

9.3.1.3 muudatuste ajalugu ja ajakohastamiste põhjendused;

9.3.1.4 läbivaatamise kuupäev ja järgmise plaanilise ajakohastamise kuupäev;

9.3.1.5 levitamise ja kinnitamise logi viited.

9.3.2 Põhikoopiat tuleb säilitada ISMS-i dokumendihoidlas versioonihalduse all.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat tuleb tõlgendada koos järgmiste dokumentidega:

10.1.1 P1 – Infoturbe poliitika: määratleb lubatud kasutuse aluseks olevad käitumisootused ja tippjuhtkonna pühendumuse.

10.1.2 P4 – Juurdepääsukontrolli poliitika: määratleb kasutajate, süsteemide ja andmete juurdepääsuga seotud õigused ja load ning jõustab vahetult lubatud kasutuse piirid.

10.1.3 P6 – Riskijuhtimise poliitika: käsitleb käitumisega seotud riske ning toetab kasutajate tegevusest tulenevate ohtudega seotud seire- ja käsitlustegevusi.

10.1.4 P7 – Tööle asumise ja töösuhte lõpetamise poliitika: tagab, et lubatud kasutuse tingimused kinnitatakse tööle asumisel ning tühistatakse töösuhte lõppemisel.

10.1.5 P9 – Kaugtöö poliitika: laiendab lubatud kasutuse nõuded kaug- ja hübriidtöö keskkondadele.

10.2 Need seotud poliitikad moodustavad käitumusliku, tehnilise ja lepingulise juhtimise jaoks kihilise kaitsemudeli.

11. Viitestandardid ja raamistikud

11.1 Käesolev lubatud kasutuse poliitika (AUP) on kooskõlas rahvusvaheliselt tunnustatud standardite ja õigusraamistikega, et tagada jõustatavad, auditikõlblikud ja riskipõhised käitumiskontrollid kogu digitaalse ja füüsilise infosüsteemide kasutuse ulatuses.

11.2 ISO/IEC 27001:2022

11.2.1 Punkt 5.10 – Teabe ja muude seotud varade lubatud kasutus: käesolev poliitika täidab otseselt nõude määratleda, edastada ja rakendada reeglid, mis reguleerivad IT-vahendite asjakohast kasutust.

11.2.2 Lisa A kontrollimeede 6.1 – Vastutus infoturbe eest: määratleb selged vastutused kasutajate käitumise ja vastavuse järelevalve osas.

11.2.3 Lisa A kontrollimeede 6.2 – Infoturbeteadlikkus, haridus ja koolitus: AUP rakendamisse on lõimitud koolitus ja poliitika kinnitamise protsessid.

11.2.4 Lisa A kontrollimeede 8.1 – Kasutaja lõppseadmed ja 8.12 – Andmekao vältimine: käsitleb lubatud käitumist kasutajaseadmetes ning reguleerib tegevusi, mis võivad viia andmete avalikustumise või andmelekkega seotud juhtumiteni.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Mobiilseadmete juurdepääsukontroll) ja AC-20 (Väliste infosüsteemide kasutamine): käesolev poliitika määratleb kasutajate kohustused ja piirangud BYOD-i ja kolmanda osapoole süsteemidele juurdepääsu korral.

11.3.2 PL-4 (Käitumisreeglid): sätestab üksikasjalikud lubatud kasutuse nõuded, mis on kooskõlas käesoleva poliitikaga.

11.3.3 AT-2 (Infoturbeteadlikkuse koolitus): toetatud kasutajakoolituse ja dokumenteeritud poliitika kinnitamise kaudu.

11.3.4 AU-2 (Auditisündmused) ja AU-12 (Auditiandmete genereerimine): rakendamine tugineb kasutajate tegevuse seirele ja rikkumiste kohta teavituste andmisele.

11.4 ELi GDPR (2016/679)

11.4.1 Artikkel 5(1)(f): nõuab isikuandmete turvalisuse ja tervikluse tagamist; käesolev poliitika vähendab inimkäitumisest ja loata kasutusest tulenevaid riske.

11.4.2 Artikkel 32: nõuab tehnilisi ja korralduslikke meetmeid, näiteks käitumiskontrolle ja kasutuspiiranguid, et kaitsta isikuandmeid.

11.4.3 Põhjendus 39: rõhutab vajadust tagada, et andmetele pääsevad ligi ja neid kasutavad õiguspäraselt ainult volitatud isikud.

11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a–d): nõuab operatiivpoliitikaid ja koolitust süsteemide turvaliseks kasutamiseks, mida käesolev AUP tagab käitumise, seire ja rakendamisprotsesside määratlemise kaudu.

11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 5: käesolev poliitika toetab IKT-riskijuhtimise raamistikku, määratledes inimese ja süsteemi koostoime reeglid ning minimeerides käitumisest tulenevat küberriski.

11.7 COBIT 2019

11.7.1 APO07 – Hallatud personal: jõustab kasutajate vastutused ja teadlikkuse kogu töötaja elutsükli jooksul.

11.7.2 BAI05 – Hallatud organisatsiooniline muudatus: lõimib lubatud kasutuse juhtimise kasutajate käitumist mõjutavatesse muudatusprotsessidesse.

11.7.3 DSS05 – Hallatud turvateenused: toetab kasutajate tegevuse seiret, käitumisteavitusi ja automatiseeritud reageerimismehhanisme.

11.7.4 MEA01 – Tulemuslikkuse ja vastavuse seire, hindamine ja analüüs: poliitika määratleb mõõdikud ja mehhanismid kasutajate vastavuse kontrollimiseks käitumisootustele.