					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P03S					Dokumendi pealkiri: **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**

Kooskõla asjakohaste standardite ja regulatsioonidega

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 5	Asjakohane poliitika üldise ulatuse ja rakendamise seisukohalt
ISO/IEC 27002:2022	5.10, 5.11, 5	Juhised lubatud kasutuse nõuete ja kontrollimeetmete kohta
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Hõlmab süsteemide ja seadmete kasutamist, seiret ning kasutajate koolitamist
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5(1)(f), 32	Andmete terviklus ja konfidentsiaalsus ning turvameetmed
ELi NIS2 direktiiv	Artikkel 21(2)(b)	Nõuab asjakohaseid turbe- ja lubatud kasutuse põhimõtteid
ELi DORA määrus	Artikkel 9	IKT-riskijuhtimise poliitika, kontrollimeetmed ja rakendamine
COBIT 2019	DSS05, BAI	Turbeteenused ja teadmushaldus

1. Eesmärk

1.1. Käesolev poliitika määratleb ettevõtte antud süsteemide, seadmete, internetiühenduse, e-posti, pilveteenuste ning äritegevuseks kasutatavate isiklike seadmete lubatud, vastutustundliku ja turvalise kasutamise.

1.2. See tagab, et isikud mõistavad organisatsiooni IT-ressursside kasutamisel oma kohustusi ning kaitsevad andmete terviklust, privaatsust ja tegevuse järjepidevust.

1.3. Käesolev poliitika toetab vastavust standardile ISO/IEC 27001:2022, kehtestades selged nõuded kasutajate käitumisele kooskõlas õiguslike, lepinguliste ja regulatiivsete nõuetega.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigile isikutele, kes pääsevad ligi ettevõtte süsteemidele või andmetele, haldavad neid või kasutavad neid, sealhulgas:

2.1.1. töötajad ja töövõtjad

2.1.2. ajutised töötajad ja praktikandid

2.1.3. välised IT-teenuse osutajad

2.2. Poliitika hõlmab:

2.2.1. ettevõttele kuuluvaid arvuteid, telefone ja tahvelarvuteid

2.2.2. äritegevuseks heaks kiidetud isiklikke seadmeid (BYOD)

2.2.3. ettevõtte võrke, pilveplatvorme ja tarkvarateenuseid

2.2.4. internetiühendust, e-posti süsteeme, ühiskasutatavat salvestusruumi ja ärirakendusi

2.3. Käesolev poliitika kehtib kõigis töökeskkondades — kohapeal, kaugtööl ja hübriidtööl — ning kogu tööaja jooksul.

3. Eesmärgid

3.1. Määratleda, mida loetakse IT-süsteemide lubatud ja lubamatuks kasutamiseks.

3.1.1. Vähendada väärkasutuse, volitamata juurdepääsu või pahavaraga nakatumisega seotud turberiske.

3.1.2. Kaitsta äriandmeid, klienditeavet ja ettevõtte mainet.

3.1.3. Kehtestada rakendatavad reeglid ja tagada kõigi kasutajate vastutus.

3.1.4. Toetada seiret ja vastavuse kontrolli, et tuvastada rikkumised varakult ja rakendada parandusmeetmeid.

4. Rollid ja vastutusalad

4.1. Tegevjuht

4.1.1. Kinnitab käesoleva poliitika ning vastutab selle eest, et poliitika rakendamiseks oleksid olemas vajalikud ressursid ja volitused.

4.1.2. Vaatab läbi ja kinnitab kõik erandid käesolevast poliitikast.

4.2. IT-juht või väline IT-teenuse osutaja

4.2.1. Hoiab ajakohasena heaks kiidetud tarkvara ja riistvara loetelud.

4.2.2. Seadistab seadmed nii, et oleks tagatud lubatud kasutuse reeglite jõustamine (nt sisufiltreerimine, juurdepääsu logimine).

4.2.3. Seirab kasutamist võimalike rikkumiste tuvastamiseks ja uurib intsidente.

4.2.4. Tagab, et äritegevuseks kasutatavad isiklikud seadmed (BYOD) on volitatud ja turvaliselt seadistatud.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Iga-aastane läbivaatamine

9.1.1. IT-juht peab käesoleva poliitika vähemalt kord aastas läbi vaatama ning tegevjuht peab andma lõpliku kinnituse, et tagada poliitika vastavus tehnoloogia kasutusmustritele, uutele riskidele ja vastavuskohustustele.

9.2. Vahepealse läbivaatamise alused

9.2.1. Läbivaatamine tuleb teha ka järgmiste asjaolude korral:

9.2.2. uued süsteemid või tehnoloogiad (nt uus pilveteenus või lõppseadme platvorm)

9.2.3. olulised poliitikarikkumised

9.2.4. ajakohastatud õigusnõuded või lepingutingimused, mis mõjutavad IT kasutamist

9.3. Muudatuste dokumenteerimine

9.3.1. Kõik muudatused tuleb registreerida versioonilogis, mis sisaldab vähemalt järgmist:

9.3.1.1. versiooni number

9.3.1.2. läbivaatamise kuupäev

9.3.1.3. muudatuste kokkuvõte

9.3.1.4. kinnitaja

9.4. Poliitika teatavaks tegemine

9.4.1. Käesoleva poliitika muudetud versioonid tuleb edastada kõigile asjakohastele kasutajatele. Töötajad peavad kinnitama selle kättesaamist ja mõistmist osana oma infoturbealase teadlikkuse kohustustest.

10. Seotud poliitikad ja seosed

10.1. Käesolev poliitika toimib koos mitme teise SME poliitikaga, et tagada turbealaste vastutuste terviklik käsitlus:

10.1.1. P4S – Juurdepääsukontrolli poliitika: määratleb lubatud kasutuse ja kontopiirangute tehnilise ning menetlusliku rakendamise.

10.1.2. P8S – Infoturbe teadlikkuse ja koolituse poliitika: annab kasutajatele juhised lubatud kasutuse piiride ja teatamiskohustuste kohta.

10.1.3. P9S – Kaugtöö poliitika: reguleerib ettevõtte süsteemide kasutamist väljaspool kontorit või kodukeskkonnas.

10.1.4. P17S – Andmekaitse ja privaatsuspoliitika: kehtestab isikuandmete töötlemise reeglid, mis on seotud lubatud kasutuse seire ja BYOD kasutamisega.

10.1.5. P30S – Intsidendihalduse poliitika: reguleerib lubatud kasutuse tingimuste väärkasutuse või rikkumiste uurimise ja neile reageerimise korda.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 5.10 – Nõuab, et organisatsioon määratleks teabevarade lubatud kasutuse ja tagaks selle rakendamise.

11.2. ISO/IEC 27002

11.2.1. Kontrollimeede 5.10 – Annab juhised süsteemide lubatud kasutuse kohta, sealhulgas lubatud ja keelatud käitumise osas.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Käsitleb süsteemide kasutamise kontrolli, sealhulgas isiklike seadmete kasutamist.

11.3.2. AC-20 – Nõuab väliste süsteemide volitamist ja seiret.

11.3.3. AT-2 – Rõhutab kasutajate koolitamist lubatud kasutuse tavade osas.

11.4. ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1. Artikkel 5(1)(f) – Nõuab isikuandmete tervikluse ja konfidentsiaalsuse tagamist, mida kasutajate väärkasutus võib kahjustada.

11.4.2. Artikkel 32 – Nõuab süsteemide ja andmete kaitsmiseks tehniliste ja korralduslike meetmete rakendamist.

11.5. ELi NIS2 direktiiv

11.5.1. Artikkel 21(2)(b) – Nõuab asjakohaseid turbepoliitikaid, sealhulgas lubatud kasutuse reegleid, et vähendada küberohte.

11.6. ELi DORA määrus

11.6.1. Artikkel 9 – Nõuab IKT-riskijuhtimise poliitikaid, mis hõlmavad kasutuskontrolle ja rakendusmehhanisme.

11.7. COBIT 2019

11.7.1. DSS05 – Turbeteenuste juhtimine: rõhutab kasutajate käitumise poliitikapõhist kontrolli.

11.7.2. BAI08 – Teadmushaldus: käsitleb teadlikkust poliitikast tulenevatest kohustustest ja lubatud kasutuse alast koolitust.