					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P20S					Dokumendi pealkiri: **Lõppseadmete kaitse - pahavarapoliitika**							
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/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Pahavarakaitse operatiivsed kontrollid
ISO/IEC 27002:2022	Kontroll 8	Lõppseadmete kaitse kontrollimeetmed
NIST SP 800-53 Rev.5	SI-3, SI-4	Pahatahtliku koodi vastased kaitsemeetmed ja intsidentidele reageerimine
EL NIS2	Artikkel 21(2)(d), (e)	Pahavarakaitse ja riskijuhtimine olulistele ja tähtsatele üksustele
EL DORA	Artikkel 10(1), 15	Operatsiooniline toimepidevus ja kolmandate osapoolte kontroll
COBIT 2019	DSS05.02, DSS05.04	Lõppseadmete ja võrkude kaitse ning seire
EL GDPR	Artikkel 32(1)(b), 33	Tehnilised ja korralduslikud meetmed ning isikuandmetega seotud rikkumisest teatamine

1. Eesmärk

1.1 Käesolev poliitika kehtestab minimaalsed tehnilised, protseduurilised ja käitumuslikud nõuded kõigi lõppseadmete, näiteks sülearvutite, lauaarvutite, mobiilseadmete ja teisaldatavate andmekandjate, kaitsmiseks pahatahtliku koodi eest, sealhulgas viiruste, lunavara, nuhkvara, rootkit'ide ja muude pahavaraohtude eest.

1.2 Poliitika eesmärk on tagada, et lõppseadmed oleksid kasutusele võetud, hallatud ja kasutatud viisil, mis vähendab pahavaraga nakatumise, selle leviku ja süsteemide kompromiteerimise riski.

1.3 Organisatsioon tunnistab, et lõppseadmed on levinud pahavara sisenemispunktid ning seetõttu tuleb neid kõvendada, seirata ja kaitsta mitmekihilise kaitse põhimõtte kohaselt.

1.4 Poliitika toetab organisatsiooni ISO/IEC 27001:2022 sertifitseerimise eesmärke ning on kooskõlas isikuandmete kaitse üldmääruse (GDPR), NIS2 direktiivi, digitaalse operatsioonilise toimepidevuse määruse (DORA) ja muude asjakohaste raamistikuga.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmistele objektidele:

2.1.1 kõik organisatsiooni lõppseadmed, sealhulgas lauaarvutid, sülearvutid, tahvelarvutid, mobiiltelefonid ja müügipunktisüsteemide (POS) terminalid

2.1.2 isiklikud seadmed, mida kasutatakse põhiliste ärirakenduste või andmete kasutamiseks oma seadme kasutamise (BYOD) raames

2.1.3 eemaldatavad salvestusseadmed, näiteks USB-mäluseadmed ja välised kõvakettad

2.1.4 kõik neil platvormidel töötavad operatsioonisüsteemid, lõppseadmete tarkvara ja sidetööriistad

2.2 Käesolev poliitika kehtib võrdselt järgmistele osapooltele:

2.2.1 sisepersonal, töövõtjad, praktikandid ja hallatud teenuse osutajad (MSP-d)

2.2.2 seadmed, mida kasutatakse ettevõtte asukohas, kaugtööl või hübriidtöö korralduses

2.2.3 pilveteenustega ühendatud või võrguühenduseta lõppseadmed, mis talletavad äriandmeid või isikuandmeid

3. Eesmärgid

3.1 Ennetada pahavaraga nakatumist ja selle levikut sisemistes süsteemides, kasutajaseadmetes ja välisühenduste kaudu

3.2 Tuvastada ja ohjeldada pahavaraga seotud ohud kiiresti, kasutades automatiseeritud lõppseadmete turbetööriistu ja määratletud eskaleerimisteid

3.3 Tagada, et äriteabele juurdepääsuks kasutatakse ainult volitatud, kaitstud ja seiratud seadmeid

3.4 Kehtestada töötajatele selged vastutused ja käitumisreeglid, et vähendada pahavaraga seotud intsidentide riski

3.5 Säilitada jälgitavad ja auditikõlblikud kirjed pahavara tuvastuste, reageerimistegevuste ja poliitika järgimise kohta

3.6 Kaitsta isikuandmeid ja äriandmeid pahavarast tingitud kompromiteerimise eest, kasutades mitmekihilise kaitse strateegiaid

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Vastutab käesoleva poliitika eest ning tagab piisavate ressursside olemasolu lõppseadmete kaitseks

4.1.2 Kiidab heaks viirusetõrjetarkvara, mobiilseadmete halduse tööriistad ja kolmandate isikute juurdepääsureeglid

4.1.3 Vaatab läbi lõppseadmetega seotud pahavaraintsidentide aruanded, mõjuhinnangute kokkuvõtted ja rikkumisteated

4.2 IT-toe teenuseosutaja / sisemine IT-administraator

4.2.1 Valib ja juurutab viirusetõrje-, pahavarakaitse- ning lõppseadme tuvastamise ja reageerimise tarkvara

4.2.2 Tagab värskenduste järjepideva rakendamise ja logide säilitamise

4.2.3 Reageerib pahavarateavitustele, isoleerib nakatunud süsteemid ja viib läbi puuduste kõrvaldamise

4.2.4 Rakendab kontrollimeetmeid USB-seadmete ja väliste seadmete kasutamise üle

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastase läbivaatamise nõue

9.1.1 Käesolev poliitika tuleb vähemalt üks kord aastas ametlikult läbi vaadata tegevjuhi poolt koostöös IT-toe teenuseosutaja ja andmekaitsekoordinaatoriga

9.2 Sündmuspõhised ajakohastamised

9.2.1 Poliitikat tuleb ajakohastada ka järgmistel juhtudel:

9.2.1.1 organisatsiooni kasutatavaid lõppseadmeid sihib uus oluline pahavaraoht või ulatuslik puhang

9.2.1.2 viirusetõrje- või lõppseadme tuvastamise ja reageerimise tööriistu muudetakse, uuendatakse või asendatakse

9.2.1.3 pahavaraintsident toob esile puudused poliitika kohaldamisalas või rakendamises

9.2.1.4 õiguslikke või regulatiivseid nõudeid, näiteks GDPR-i, DORA-t või NIS2-te, ajakohastatakse

9.3 Versioonihaldus ja teavitamine

9.3.1 Kõik poliitikamuudatused tuleb dokumenteerida koos versiooninumbri, kuupäeva ja muudatuste kokkuvõttega

9.3.2 Töötajaid tuleb ajakohastustest teavitada, eriti kui need muudavad tegevuslikke või käitumuslikke nõudeid

9.3.3 Varasemaid versioone tuleb auditite toetamiseks säilitada poliitikaarhiivis vähemalt 3 aastat

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat tuleb rakendada koos järgmiste VKE poliitikatega:

10.1.1 P9S – kaugtööpoliitika: tagab, et lõppseadmete kaitse nõudeid rakendatakse väljaspool ettevõtte asukohta või hübriidkorralduses kasutatavatele seadmetele

10.1.2 P12S – varahalduse poliitika: toetab kõigi lõppseadmete jälgimist ja kontrolli, tagades, et kasutatakse ainult volitatud ja kaitstud seadmeid

10.1.3 P17S – andmekaitse ja privaatsuse poliitika: kinnistab pahavara vältimise kui põhikontrollimeetme isikuandmete ja tundlike andmete kaitseks kompromiteerimise eest

10.1.4 P22S – logimis- ja seirepoliitika: kehtestab nõuded pahavarasündmuste logimiseks ja teavituste nähtavuse säilitamiseks varajase reageerimise eesmärgil

10.1.5 P30S – intsidentidele reageerimise poliitika: määrab kindlaks eskaleerimise, ohjeldamise ja välise teavitamise sammud, kui pahavara põhjustab andmete kompromiteerimise või tegevushäire

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab operatiivsete kontrollimeetmete rakendamist selliste riskide vähendamiseks nagu pahavararünnakud

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.7 – kirjeldab pahavara vastaseid kontrollipraktikaid, sealhulgas viirusetõrjet, reaalajaskannimist, värskendusi ja kasutajakoolitust

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – nõuab pahatahtliku koodi vastaste kaitsemehhanismide juurutamist kõigis lõppseadmetes

11.3.2 SI-4 – nõuab lõppseadme tasemel ohtude ja teavituste seiret, tuvastamist, analüüsi ja reageerimist

11.4 EL GDPR

11.4.1 Artikkel 32(1)(b) – nõuab isikuandmete kaitseks tehnilisi ja korralduslikke kontrollimeetmeid, näiteks viirusetõrjet

11.4.2 Artikkel 33 – kohustab rikkumisest teatama, kui pahavara kahjustab andmete terviklust, konfidentsiaalsust või käideldavust

11.5 EL NIS2 direktiiv

11.5.1 Artikkel 21(2)(d) – nõuab meetmeid pahavaraohtude vältimiseks ja neile reageerimiseks olulistes ja tähtsates üksustes

11.5.2 Artikkel 21(2)(e) – nõuab kihilisi küberturberiskide juhtimise strateegiaid, sealhulgas lõppseadmete pahavarakaitset

11.6 EL DORA

11.6.1 Artikkel 10(1) – nõuab IKT-süsteemide kaitsmist pahavara ja muude ohtude eest operatsioonilise toimepidevuse osana

11.6.2 Artikkel 15 – kohustab finantsorganisatsioone kontrollima pahavarakaitset kolmandatest osapooltest teenuseosutajate juures

11.7 COBIT 2019

11.7.1 DSS05.02 – rõhutab kontrollimeetmeid lõppseadmete ja võrkude kaitsmiseks pahavaraohtude eest

11.7.2 DSS05.04 – toetab pahavaraga seotud turvasündmuste seiret ja teavitamist jooksva tegevuse osana