					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P20					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 regulatiivsete nõuetega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Lõppseadmete kaitse ja pahavaratõrje kontrollimeetmed on vajalikud ISMS-i eesmärkide saavutamiseks
ISO/IEC 27002:2022	Kontrollimeetmed 8.7, 8	Annab tehnilised kontrollimeetmed ja juhised pahavaratõrje, lõppseadmete kaitse ning intsidendihalduse jaoks
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Määratleb pahatahtliku koodi kaitse, tsentraliseeritud seire ja lähteseadistuse nõuded
EL GDPR	Artikkel 32	Nõuab asjakohaseid tehnilisi meetmeid isikuandmete kaitsmiseks, sealhulgas kaitset pahavara eest
EL NIS2	Artikkel 21(2)(d)	Nõuab lõppseadme tasemel ohtude tuvastamise ja ennetusmeetmete rakendamist
EL DORA	Artikkel 9	Nõuab IKT-riskide juhtimist pahavara ja lõppseadmetest lähtuvate ohtude vastu
COBIT 2019	DSS05.01, DSS01.04, seire, hindamine ja auditeerimine	Nõuab lõppseadmete kaitse kontrollimeetmete rakendamist, seiret ja hindamist

1. Eesmärk

1.1 Käesolev poliitika sätestab kohustuslikud kontrollimeetmed ja tegevusnõuded organisatsiooni lõppseadmete, sealhulgas lauaarvutite, sülearvutite, mobiilseadmete ja serverite kaitsmiseks pahavara ja sellega seotud ohtude eest.

1.2 Poliitika kehtestab miinimumnõuded lõppseadmete kaitsele, pahavara tuvastamisele, ohjeldamisele, reageerimisele ja käitumuslikule seirele, et süsteemid säilitaksid toimepidevuse nii levinud kui ka keerukate pahavaravariantide vastu.

1.3 Poliitika toetab otseselt vastavust standardi ISO/IEC 27001:2022 punktile 8.1 ja lisa A kontrollimeetmele 8.7 ning on kooskõlas piirkondlike küberturvalisuse nõuetega GDPR-i, NIS2 ja DORA alusel.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile lõppseadmetele, sealhulgas:

2.1.1 organisatsiooni omandis olevatele või organisatsiooni hallatavatele lauaarvutitele, sülearvutitele, mobiilseadmetele ja virtuaalinstantsidele;

2.1.2 isiklikele seadmetele, mille kasutamine on BYOD-poliitika alusel lubatud, tingimusel et neile on paigaldatud MDM või lõppseadme agent;

2.1.3 serveritele ja taristuvaradele, sealhulgas pilvekeskkonnas majutatud virtuaalmasinatele ja ääretaristu seadmetele;

2.1.4 operatsioonisüsteemidele, draiveritele, kohalikele teenustele, lõppseadme agentidele ja igasse sõlme paigaldatud turbekontrollidele.

2.2 Käesolev poliitika hõlmab kõiki isikuid, kellel on halduslik, tehniline või operatiivne vastutus mis tahes lõppseadme eest, sealhulgas:

2.2.1 sisemisi töötajaid ja töövõtjaid;

2.2.2 hallatud teenusepakkujaid (MSP), sisseostetud töölauatoe teenuse osutajaid ja kolmandate osapoolte IT-administraatoreid;

2.2.3 kasutajaid, kellel on õigus kasutada kaasaskantavaid süsteeme, VPN-toega sülearvuteid või mobiilset juurdepääsu organisatsiooni võrkudele.

2.3 Käesoleva poliitika ohuulatus hõlmab muu hulgas järgmist:

2.3.1 viirused, ussid, troojalased, lunavara, nuhkvara, rootkitid, reklaamvara, klahvilogijad ja botivõrgud;

2.3.2 failivaba pahavara, nullpäeva ärakasutused, õiguste eskaleerimise pahavara ja brauseri ekspluateerimiskomplektid;

2.3.3 eemaldatava andmekandja, andmepüügivektorite, automaatsete allalaadimiste või USB-põhiste rünnete kaudu edastatud pahatahtlik kood.

3. Eesmärgid

3.1 Kaitsta lõppseadmete terviklust, käideldavust ja konfidentsiaalsust ning nende töödeldavaid andmeid usaldusväärse pahavara ennetamise, tuvastamise ja reageerimise kaudu.

3.2 Tõkestada pahatahtliku koodi käivitamine või levik organisatsiooni võrkudes, rakendades tehnilisi kaitsemeetmeid, lähteseadistuse kõvendamist ja reaalaja telemeetriat.

3.3 Lõimida lõppseadmete kaitse teiste ISMS-i kontrollimeetmetega, sealhulgas haavatavuste halduse, juurdepääsukontrolli, logimise ja seire ning intsidentidele reageerimisega.

3.4 Tagada lõppseadmete pidev nähtavus tsentraalselt hallatavate kaitseplatvormide kaudu, sealhulgas viirusetõrje-/pahavaratõrje agendid, lõppseadme tuvastus ja reageerimine ning SIEM-i telemeetria.

3.5 Täita õiguslikud, regulatiivsed ja standardipõhised nõuded, mis kohustavad tagama lõppseadmete turbe, näiteks GDPR artikkel 32, NIS2 artikkel 21 ja DORA artikkel 9.

3.6 Määratleda vastutavad rollid, rakendada paikamise ja teavitustele reageerimise SLA-d ning tagada auditivalmidus dokumentatsiooni ja aruandluse kaudu.

4. Rollid ja vastutused

4.1 Infoturbejuht

4.1.1 Vastutab käesoleva poliitika eest ja tagab selle kooskõla ISMS-i ning üldise turbestrateegiaga.

4.1.2 Vaatab kord kvartalis läbi lõppseadmete kaitse mõõdikud, intsidenditrendid ja tööriistade tõhususe.

4.1.3 Kiidab heaks lõppseadmete katvusega seotud erandid ja jääkriski aktsepteerimised.

4.2 Lõppseadmete turbe juht / turbeoperatsioonide keskuse juht

4.2.1 Haldab lõppseadmete kaitsesüsteeme, näiteks AV-, EDR- ja MDM-lahendusi.

4.2.2 Teostab järelevalvet poliitika rakendamise, ohtude tuvastamise häälestamise ja reageerimise tööjuhiste üle.

4.2.3 Hoiab ajakohasena katvusstatistika, pahavaraintsidentide logid ja teavituste konfiguratsiooni lähteseadistused.

[... 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 kord aastas või juhul, kui:

9.1.1 toimub ulatuslik pahavarakampaania või lõppseadmete turbeintsident;

9.1.2 uued ohutüübid, näiteks failivaba pahavara või lunavara variandid, nõuavad tuvastamise või reageerimise strateegiate ajakohastamist;

9.1.3 lõppseadmete kaitse platvormid või agentide arhitektuurid muutuvad oluliselt;

9.1.4 lõppseadmete kontrollimeetmeid mõjutavaid õiguslikke või regulatiivseid nõudeid ajakohastatakse.

9.2 Läbivaatamise algatab lõppseadmete turbe juht ning see koordineeritakse infoturbejuhi, õigus-, riski- ja auditifunktsioonidega.

9.3 Heakskiidetud muudatused tuleb dokumenteerida ISMS-i dokumentide kontrolli registris, neile tuleb määrata uus versioonitähis ning neist tuleb teavitada kõiki mõjutatud osapooli.

9.4 Asendatud versioonid tuleb arhiveerida, piirata neile juurdepääsu ning säilitada auditijälje tervikluse tagamiseks vastavalt ISMS-i säilitustähtaegadele.

10. Seotud poliitikad ja seosed

10.1 P1 - Infoturbepoliitika. Määratleb süsteemide, andmete ja võrkude kaitse aluspõhimõtted. Käesolev poliitika rakendab neid põhimõtteid lõppseadmete tasandil tehniliste ja protseduuriliste pahavaratõrje kontrollimeetmete kaudu.

10.2 P4 - Juurdepääsukontrolli poliitika. Määratleb kasutajate juurdepääsupiirangud, mida rakendatakse ka lõppseadmete tasandil, sealhulgas kaitse õiguste eskaleerimise ja kontrollimata tarkvara autoriseerimata paigaldamise vastu.

10.3 P5 - Muudatuste haldamise poliitika. Tagab, et lõppseadmete kaitse tarkvara, poliitikareeglite või agentide konfiguratsioonide muudatused alluvad heakskiidule ja kontrollitud juurutusprotsessidele.

10.4 P12 - Varahalduse poliitika. Määrab vara klassifitseerimise ja registri lähtetaseme, mis on vajalik lõppseadmete nähtavuse, paikamiskatvuse ja pahavaratõrje kohaldamisala määratlemiseks.

10.5 P22 - Logimise ja seire poliitika. Võimaldab lõppseadmete teavituste, agentide töökorras oleku ja ohuteabe lõimimist tsentraliseeritud SIEM-süsteemidesse reaalaja tuvastamise ja kohtuekspertiisi jälgitavuse tagamiseks.

10.6 P30 - Intsidentidele reageerimise poliitika (P30). Seob lõppseadmetel põhinevad pahavaraintsidendid standardiseeritud ohjeldamise, kõrvaldamise, uurimise ja taaste töövoogudega koos määratud rollide ja eskaleerimislävenditega.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001:

11.1.1 Punkt 8.1 - Operatiivne planeerimine ja kontroll: nõuab tehniliste kontrollimeetmete, sealhulgas lõppseadmete kaitsemeetmete rakendamist ISMS-i eesmärkide saavutamiseks.

11.2 ISO/IEC 27002:2022 - Kontrollimeetmed 8.7, 8:

11.2.1 Annab üksikasjalikud tehnilised juhised pahavaratõrjemeetmete, turvalise tarkvarajuurutuse, seire ja intsidendivalmiduse kohta lõppseadmete keskkondades.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Pahatahtliku koodi kaitse: nõuab pahavaratõrje tööriistade kasutamist koos reaalaja, juurdepääsupõhise skannimise ja käitumusliku analüüsiga.

11.3.2 SI-4 - Süsteemide seire: toetab telemeetria lõimimist tsentraliseeritud tuvastusplatvormidega.

11.3.3 CM-6 - Konfiguratsiooniseaded: tugevdab lõppseadmete lähteseadistuse kontrollimeetmeid, sealhulgas kaitseagentide rakendamist.

11.4 EL GDPR (2016/679):

11.4.1 Artikkel 32 - Töötlemise turvalisus: nõuab organisatsioonidelt asjakohaste tehniliste meetmete rakendamist isikuandmete kaitsmiseks, sealhulgas kaitset pahavaraohtude eest.

11.5 EL NIS2 direktiiv (2022/2555):

11.5.1 Artikkel 21(2)(d): kohustab üksusi rakendama ohtude tuvastamise ja ennetamise meetmeid, sealhulgas pahavaratõrje mehhanisme lõppseadmete tasandil.

11.6 EL DORA (2022/2554):

11.6.1 Artikkel 9 - IKT-riskide juhtimise nõuded: nõuab finantsüksustelt kaitsemeetmete rakendamist pahavara ja lõppseadmetest lähtuvate ohtude ennetamiseks, tuvastamiseks ja neile reageerimiseks.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Kaitse pahavara vastu: nõuab pahavara tuvastamist ja maandamist kõigis organisatsiooni lõppseadmetes.

11.7.2 DSS01.04 - Käideldavuse ja mahu haldamine: tagab, et pahavaratõrje on tasakaalus süsteemi jõudluse ja talitluspidevusega.

11.7.3 MEA03 - Vastavuse seire, hindamine ja auditeerimine: nõuab lõppseadmete kontrollimeetmete ja kaitse tõhususe perioodilist auditeerimist.