					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P22S					Dokumendi pealkiri: **logimis- ja seirepoliitika**							
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/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Operatiivsed kontrollid, sh logimine
ISO/IEC 27002:2022	Kontrollid 8.15, 8.16, 8.17	Sündmuste logimine, logide kaitse ja seire
NIST SP 800-53 Rev.5	AU-2 kuni AU-12, SI-4	Auditilogide sisu ja läbivaatamine, säilitamine, anomaaliatuvastus, teavitused
ELi GDPR	Artiklid 5(1)(f), 32, 33	Isikuandmete konfidentsiaalsus ja terviklus, tehnilised meetmed ning rikkumistest teavitamine
ELi NIS2	Artiklid 21(2)(d), 23	Anomaaliate tuvastamise logimismehhanismid ja intsidentidest teatamine 24 tunni jooksul
ELi DORA	Artiklid 10, 15	Digitaalne tegevuskerksus, teenuseosutajate seire ja logimine
COBIT 2019	DSS01.03, DSS05.02	Tegevuste jälgitavus ning kaitse logimise ja seire kaudu

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud logimise ja seire kontrollid, et tagada organisatsiooni IT-süsteemide turvalisus, vastutus ja töökindel toimimine.

1.2 Poliitika määratleb logitavate sündmuste liigid, logide säilitamise korra, logide läbivaatamise korra ning töötajate ja teenuseosutajate vastutuse.

1.3 Logimine ja seire toetavad ohtude tuvastamist, õigusnormidele vastavuse tagamist, intsidentidele reageerimist ja kohtuekspertiisi analüüsi.

1.4 Käesolev poliitika võimaldab organisatsioonil täita ISO/IEC 27001 operatiivsete kontrollide nõudeid ning toetab pidevat auditivalmidust, klientide usaldust ja vastavust GDPR-i, NIS2 ja DORA nõuetele.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile organisatsiooni süsteemidele ja kasutajatele, sealhulgas:

2.1.1 tööjaamadele, sülearvutitele, serveritele, tulemüüridele, lülititele, ruuteritele ja traadita pääsupunktidele

2.1.2 äritegevuses kasutatavatele pilveteenustele (nt e-post, failisalvestus, varukoopiad, koostöötööriistad)

2.1.3 viirusetõrjetarkvara, rakenduste, operatsioonisüsteemide ja võrguseadmete logimisfunktsioonidele

2.1.4 kõigile süsteeme kasutavatele või haldavatele töötajatele, töövõtjatele ja hallatud teenuse osutajatele (MSP)

2.1.5 kõigile asukohtadele, kus kasutatakse ettevõtte IT-süsteeme, sealhulgas kaugtöö-, hübriidtöö- või oma seadme kasutamise (BYOD) keskkondadele

2.2 Poliitika kohaldub ka kolmandate osapoolte teenuste loodud logidele, kui organisatsioonil on haldusjuurdepääs või lepinguline auditeerimisõigus.

3. Eesmärgid

3.1 Tagada süsteemitegevuste logimine, sealhulgas autentimine, konfiguratsioonimuudatused, juurdepääs tundlikele andmetele ja turvateavitused.

3.2 Säilitada turvalised ja täpsed logid poliitikarikkumiste, süsteemivigade või loata tegevuste tuvastamiseks.

3.3 Võimaldada logide kiire läbivaatamine intsidentide, uurimiste ja auditite käigus.

3.4 Toetada aja sünkroniseerimist, et tagada logiandmete terviklus ja omavaheline korreleerimine.

3.5 Kaitsta logisid rikkumise, kaotsimineku või enneaegse kustutamise eest.

3.6 Täita süsteemse vastutuse, jälgitavuse ja rikkumistele reageerimisega seotud õiguslikud ja regulatiivsed kohustused.

4. Rollid ja vastutused

4.1 tegevjuht

4.1.1 kiidab käesoleva poliitika heaks ja tagab selle rakendamise kõigis ärisüsteemides

4.1.2 vaatab läbi IT-funktsiooni või andmekaitse eest vastutava isiku esitatud kõrge tõsidusega teavitused ja olulised auditileiud

4.1.3 kiidab heaks erandid, kui logimist või säilitamist ei ole tehniliselt võimalik rakendada

4.2 IT-toe teenuseosutaja / sisemine IT-vastutaja

4.2.1 rakendab ja seadistab logimise operatsioonisüsteemidele, võrguseadmetele, viirusetõrjevahenditele ja peamistele rakendustele

4.2.2 tagab logide säilitamise, varundamise ja muutmise eest kaitsmise

4.2.3 vaatab logid plaanipäraselt läbi ning uurib kahtlast või loata tegevust

4.2.4 haldab teavitussüsteeme, mis tuvastavad anomaalset käitumist või sissetungi tunnuseid

[... 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 Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata tegevjuhi poolt IT-toe teenuseosutaja ja andmekaitse eest vastutava isiku toel.

9.2 Läbivaatamise alused

9.2.1 Plaaniväline läbivaatamine tuleb teha järgmiste asjaolude ilmnemisel:

9.2.1.1 logidega seotud leiud sise- või välisaudititest

9.2.1.2 turvaintsidendid, mille puhul logid puudusid, olid rikutud või ebapiisavad

9.2.1.3 olulised muudatused IT-taristus (nt üleminek pilvepõhistele logimisplatvormidele)

9.2.1.4 õiguslike või regulatiivsete kohustuste ajakohastused (nt GDPR, NIS2, DORA)

9.3 Versioonihaldus

9.3.1 Kõik käesoleva poliitika muudatused tuleb registreerida koos versiooninumbri, kuupäeva ja muudatuste kokkuvõttega

9.3.2 Varasemad versioonid tuleb arhiveerida ja säilitada vähemalt 3 aastat

9.3.3 Ajakohastatud poliitikad tuleb edastada mõjutatud sidusrühmadele, eelkõige neile, kellel on süsteemitaseme juurdepääs

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toetab otseselt järgmisi VKE infoturbepoliitikaid ja on nendega seotud:

10.1.1 P17S – Andmekaitse- ja privaatsuspoliitika: tagab, et isikuandmeid sisaldavaid logiandmeid hallatakse tervikluse, säilitamise ja juurdepääsu kaitsemeetmetega kooskõlas GDPR-i nõuetega.

10.1.2 P21S – Võrguturbe poliitika: loob aluse tulemüüride, traadita juurdepääsu, VPN-ide ja segmenteerimise seirega seotud logide kogumiseks.

10.1.3 P24S – Turvalise arenduse poliitika: tagab, et rakenduste logid (nt sisselogimiskatsed, vead ja erandid) on tarkvara kavandamisse ja käitamisse sisse ehitatud.

10.1.4 P30S – Intsidentidele reageerimise poliitika: tugineb täpsetele ja täielikele logiandmetele infoturbesündmuste tuvastamisel, analüüsimisel ja neile reageerimisel.

10.1.5 P23S – Aja sünkroniseerimise poliitika: tagab kõigis süsteemides järjepidevad ja jälgitavad ajatemplid, võimaldades logisid uurimiste käigus korreleerida.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab infoturberiskide maandamiseks operatiivsete kontrollide rakendamist, sealhulgas logimist.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.15 – nõuab sündmuste logimist anomaaliatuvastuse ja vastutuse toetamiseks.

11.2.2 Kontroll 8.16 – nõuab logide kaitsmist rikkumise ja loata juurdepääsu eest.

11.2.3 Kontroll 8.17 – nõuab süsteemide seiret ebatavalise tegevuse tuvastamiseks ja seirekontrollide tõhususe kinnitamiseks.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 kuni AU-12 – hõlmavad auditilogide sisu, läbivaatamist, säilitamist ja automaatseid teavitusi.

11.3.2 SI-4 – nõuab süsteemianomaaliate tuvastamist ja kahtlaste sündmuste raporteerimist.

11.4 ELi GDPR

11.4.1 Artikkel 5(1)(f) – nõuab isikuandmete terviklust ja konfidentsiaalsust, mis hõlmab ka juurdepääsu logimist.

11.4.2 Artikkel 32 – kohustab rakendama tehnilisi ja korralduslikke meetmeid turvalisuse tagamiseks, sealhulgas logimist ja seiret.

11.4.3 Artikkel 33 – nõuab rikkumistest õigeaegset teavitamist, mida toetavad algpõhjuse analüüsi võimaldavad logid.

11.5 ELi NIS2 direktiiv

11.5.1 Artikkel 21(2)(d) – nõuab logimismehhanisme, mis tuvastavad anomaaliaid ja toetavad intsidentide uurimist.

11.5.2 Artikkel 23 – kohustab intsidentidest teatama 24 tunni jooksul, mis sõltub täpsetest ja õigeaegsetest logiandmetest.

11.6 ELi DORA

11.6.1 Artikkel 10 – nõuab digitaalset tegevuskerksust, sealhulgas IKT-ga seotud intsidentide jälgitavust logimise kaudu.

11.6.2 Artikkel 15 – kohustab seirama teenuseosutajaid, sealhulgas tagama juurdepääsu logidele ja nende läbivaatamise õigused.

11.7 COBIT 2019

11.7.1 DSS01.03 – nõuab süsteemitegevuste jälgitavust logimise ja seire kaudu.

11.7.2 DSS05.02 – käsitleb logimist kui olulist kontrolli pahavara ja muu loata tegevuse vastu kaitsmisel.