					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P22					Dokumendi pealkiri: **logimise ja seire 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**

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on kehtestada selged ja jõustatavad nõuded organisatsiooni IT-keskkonnas toimuvate oluliste süsteemi- ja turbesündmuste logide genereerimiseks, kaitsmiseks, läbivaatamiseks ja analüüsimiseks.

1.2 Logimine ja seire on kriitilise tähtsusega anomaaliate tuvastamise, ohtudele reageerimise, kohtuekspertiisi, auditivalmiduse ja õigusnormidele vastavuse tagamiseks. Käesolev poliitika tagab, et kõik süsteemi genereeritud sündmused logitakse, säilitatakse ja ajaliselt korreleeritakse nõuetekohase täpsusega.

1.3 Käesolev poliitika on oluline ISO/IEC 27001 punkti 8.1 ning lisa A kontrollimeetmete 8.15 (logimine), 8.16 (seire) ja 8.17 (kella sünkroniseerimine) toetamiseks ning on otseselt seotud GDPR-i, NIS2, DORA ja COBIT 2019 regulatiivsete kohustustega.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile süsteemidele, teenustele ja keskkondadele, mis talletavad, töötlevad või edastavad andmeid, mis kuuluvad infoturbe juhtimissüsteemi (ISMS) kohaldamisalasse, sealhulgas:

2.1.1 kohapealne taristu, pilveteenused (nt IaaS, PaaS, SaaS) ja hübriidkeskkonnad

2.1.2 operatsioonisüsteemid, andmebaasid, rakendused ja võrguseadmed

2.1.3 turbesüsteemid, nagu SIEM-id, tulemüürid, lõppseadmete tuvastamise ja reageerimise platvormid, VPN-kontsentraatorid ja identiteedipakkujad

2.2 Kohaldamisalasse kuuluvad järgmised sidusrühmad:

2.2.1 sisekasutajad, kellel on süsteemi- või haldusõigused

2.2.2 taristu- ja IT-operatsioonide töötajad

2.2.3 turbeoperatsioonide keskus (SOC) ja ohutuvastusmeeskonnad

2.2.4 tarkvaraarendajad ja rakenduste omanikud

2.2.5 kolmandatest osapooltest teenuseosutajad, kes haldavad logisid genereerivaid süsteeme

3. Eesmärgid

3.1 Tagada, et kõik kriitilised süsteemid genereerivad turbesündmuste logisid ja süsteemi tegevuskirjeid, mida säilitatakse kooskõlas regulatiivsete, õiguslike ja lepinguliste nõuetega.

3.2 Määratleda minimaalsed sündmustüübid ja logide sisu, mis on vajalikud loata tegevuste tuvastamiseks, kasutajate tegevuste jälgitavuse tagamiseks ja kohtuekspertiisi toetamiseks.

3.3 Rakendada kaitsemeetmed, mis hoiavad ära logide rikkumise, loata kustutamise või kontrollimatu juurdepääsu logiandmetele.

3.4 Kehtestada tsentraliseeritud logimis- ja teavitussüsteemid (nt SIEM), et koondada, korreleerida ja eskaleerida kahtlast tegevust peaaegu reaalajas.

3.5 Tagada süsteemikellade sünkroniseerimine, et võimaldada täpset süsteemidevahelist korrelatsiooni ja intsidentide analüüsi.

3.6 Võimaldada pidevat parendamist ja vastavust, lõimides logiseire auditi, riskijuhtimise ja intsidentide halduse protsessidega.

4. Rollid ja vastutused

4.1 infoturbejuht

4.1.1 Vastutab käesoleva poliitika eest ja tagab selle kooskõla organisatsiooni riskipositsiooni, auditinõuete ja ISMS-i kohustustega.

4.1.2 Kinnitab reguleeritud või kõrge riskiga süsteemide logimise kohaldamisala ning teostab järelevalvet vastavusaruandluse üle.

4.2 turbeoperatsioonide keskuse (SOC) juht

4.2.1 Käitab ja haldab tsentraliseeritud logihalduse platvorme (nt SIEM).

4.2.2 Määratleb logide koondamise reeglid, teavituste lävendid ja intsidentide esmase hindamise eskaleerimisteed.

4.2.3 Vaatab läbi igapäevased aruanded ning tagab, et anomaaliad analüüsitakse, dokumenteeritakse ja eskaleeritakse vastavalt vajadusele.

[... 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 varem järgmistel juhtudel:

9.1.1 suuremad muudatused süsteemiarhitektuuris või logimistaristus (nt SIEM-i migreerimine)

9.1.2 muudatused regulatiivsetes logimisnõuetes (nt NIS2 või DORA logimisnõuded)

9.1.3 auditite või intsidendijärgsete analüüside leiud

9.1.4 uued ohud, mis nõuavad tõhustatud seiret (nt siseohud, tarneahela kompromiteerimine)

9.2 Läbivaatamise protsessi juhib turbeoperatsioonide keskuse (SOC) juht koostöös infoturbejuhiga, riskijuhtimise, vastavusfunktsiooni ja taristumeeskondadega.

9.3 Heakskiidetud muudatused tuleb versioonihalduse all kanda ISMS-i dokumentide kontrolliregistrisse ning edastada järgmistele osapooltele:

9.3.1 kõik sidusrühmad, kes vastutavad logimissüsteemide haldamise eest

9.3.2 rakenduste ja süsteemide omanikud

9.3.3 kolmandate osapoolte teenuseosutajad, kellel on telemeetria või SIEM-i lõimimise kohustused

9.4 Kõik asendatud versioonid tuleb turvaliselt arhiveerida ning juurdepääs neile peab olema piiratud volitatud ISMS-i halduritega auditi ja õiguslike eesmärkide jaoks.

10. Seotud poliitikad ja seosed

10.1 P1 – Infoturbepoliitika. Määratleb aluspõhimõtted süsteemide ja andmete kaitseks, mille raames logimine ja seire toimivad oluliste tuvastusmeetmete ja reageerimisvõime võimaldajatena.

10.2 P4 – Juurdepääsukontrolli poliitika. Tagab, et privilegeeritud juurdepääs, kasutajate sisselogimised ja autoriseerimissündmused logitakse ning neid seiratakse väärkasutuse või anomaalse käitumise tuvastamiseks.

10.3 P5 – Muudatuste haldamise poliitika. Nõuab süsteemimuudatuste, paikade juurutamise ja konfiguratsioonivärskenduste logimist, mis võivad tekitada riski või põhjustada autoriseerimata muudatusi.

10.4 P21 – Võrguturbe poliitika. Nõuab võrgutaseme logimist (nt tulemüürilogid, IDS/IPS-i teavitused, VPN-i tegevus) ning lõimimist SIEM-iga, et tagada nähtavus liiklusanomaaliatele ja perimeetrikaitsele.

10.5 P23 – Aja sünkroniseerimise poliitika. Tagab kellaaegade ühtsuse süsteemide vahel, mis on hädavajalik usaldusväärseks logimiseks ja turbesündmuste korrelatsiooniks mitmes keskkonnas.

10.6 P30 – Intsidentidele reageerimise poliitika. Tugineb logiandmetele ja teavitusmehhanismidele turvaintsidentide tuvastamiseks, uurimiseks ja neile reageerimiseks ning säilitab kohtuekspertiisi artefaktid intsidendijärgseks läbivaatamiseks.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – operatiivne planeerimine ja kontroll: nõuab kontrollimeetmeid tegevuste seireks ning loata juurdepääsu ja süsteemi väärkasutuse vältimiseks.

11.2 ISO/IEC 27002:2022 – kontrollimeetmed 8.15, 8.16, 8.17

11.2.1 Määratleb üksikasjalikud logimisnõuded, sealhulgas millised sündmused tuleb registreerida, kuidas logisid kaitsta ja analüüsida ning kuidas tagada ajatemplite usaldusväärsus süsteemide lõikes.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 kuni AU-12: hõlmab sündmuste valikut, logimist, kaitset, auditite läbivaatamist, reageerimist auditi tõrgetele ja auditikirjete säilitamist.

11.3.2 SI-4 – süsteemide seire: nõuab aktiivset süsteemide seiret koos anomaalse tegevuse põhjal genereeritud teavitustega.

11.3.3 SC-45 – süsteemiaja sünkroniseerimine: tugevdab aja täpsust sündmuste jälgitavuse ja intsidentide korrelatsiooni tagamiseks.

11.4 EL GDPR (2016/679)

11.4.1 Artikkel 32 – töötlemise turvalisus: nõuab tehnilisi kontrollimeetmeid, näiteks logimist ja seiret, et tagada turvalisus ja vastutus, eelkõige isikuandmetele juurdepääsu korral.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(e): nõuab sündmuste logimist ja seiresüsteeme turvaintsidentide kiireks tuvastamiseks ja neile reageerimiseks.

11.6 EL DORA (2022/2554)

11.6.1 Artikkel 9 – IKT-riskide juhtimine: nõuab mehhanisme anomaalse tegevuse tuvastamiseks, intsidentide logimiseks ja kohtuekspertiisi andmete säilitamiseks.

11.6.2 Artikkel 11 – IKT talitluspidevuse plaanide testimine: rõhutab seire järjepidevust ja logide kättesaadavuse valideerimist tegevushäirete ajal.

11.7 COBIT 2019

11.7.1 DSS01.05 – turvalogide haldamine: nõuab logimisvõimekuse rakendamist kogu kriitilises taristus.

11.7.2 DSS05.04 – turbesündmuste seire: nõuab logide reaalajalähedast seiret ja analüüsi sündmuste tuvastamiseks ning neile reageerimiseks.

11.7.3 MEA03 – vastavuse seire, hindamine ja auditeerimine: nõuab logimispraktikate regulaarset läbivaatamist ja kooskõla kontrollieesmärkidega.