					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P23					Dokumendi pealkiri: **Aja sünkroniseerimise 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 standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	-
ISO/IEC 27002:2022	Kontroll 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
EL GDPR	Artikkel 32	-
EL NIS2	Artikkel 21(2)(e)	-
EL DORA	Artiklid 9, 10	-
COBIT 2019	DSS05.04, vastavuse seire, hindamine ja auditeerimine	-

1. Eesmärk

1.1 Käesoleva poliitika eesmärk on tagada, et kõik organisatsiooni süsteemid, rakendused, seadmed ja pilveteenused kasutavad ühtseid ja täpseid ajaseadeid ning sünkroniseerivad need määratud ja usaldusväärsete ajaallikatega.

1.2 Täpne aja sünkroniseerimine on hädavajalik usaldusväärseks logimiseks, turvaliseks sideks, auditi jälgitavuseks, intsidendihalduseks ja digitaalseks ekspertiisiks. Aja ebaühtlus võib põhjustada omavahel mitteseostatavaid logisid, autentimise tõrkeid ja puudulikku regulatiivset aruandlust.

1.3 Käesolev poliitika toetab standardi ISO/IEC 27001 lisa A kontrolli 8.17 ja seotud rahvusvahelisi standardeid, tagades aja täpsuse ning kellatriivi tuvastamise kogu organisatsiooni IT-taristus.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõik taristukomponendid, sealhulgas serverid, tööjaamad, võrguseadmed, tulemüürid ja asjade interneti (IoT) süsteemid;

2.1.2 virtuaal- ja pilvekeskkonnad (nt AWS, Azure, Google Cloud);

2.1.3 kõik süsteemid, mis osalevad logimises, autentimises, tehingute töötlemises või turbesündmuste korreleerimises;

2.1.4 organisatsiooni töötajad, töövõtjad ja kolmandatest osapooltest teenuseosutajad, kes vastutavad ajakriitiliste süsteemide eest.

2.2 Kohaldamisalasse kuuluvad kõik süsteemid, mis loovad või kasutavad ajatempliga kirjeid, näiteks logikirjed, teavitused, kasutajate tegevuskirjed või digitaalse ekspertiisi tõendid.

3. Eesmärgid

3.1 Määratleda ühtne ja tsentraliseeritud aja sünkroniseerimise arhitektuur, kasutades heakskiidetud NTP-allikaid või samaväärseid lahendusi.

3.2 Tagada, et kõik süsteemid sünkroniseerivad oma kellad kindlaksmääratud intervallidega ning et mis tahes triiv tuvastatakse ja korrigeeritakse automaatselt või minimaalse käsitsi sekkumisega.

3.3 Säilitada kellade täpsus hübriid-, kohapealsetes ja pilvekeskkondades, et võimaldada:

3.3.1 usaldusväärset sündmuste korreleerimist ja intsidendihaldust;

3.3.2 õigusnormidele vastavust selliste standardite ja regulatsioonide alusel nagu ISO 27001, GDPR, NIS2 ja DORA;

3.3.3 kaitset kordusrünnete ja ajapõhiste autentimistõrgete eest.

3.4 Kehtestada selged rollid, erandite haldamise protseduurid ja auditimehhanismid, et tagada poliitika rakendamine.

3.5 Tagada, et ajaga seotud anomaaliad logitakse, nende kohta väljastatakse teavitused ja need eskaleeritakse, kui need ületavad lubatud hälbeid.

4. Rollid ja vastutused

4.1 infoturbejuht

4.1.1 Vastutab käesoleva poliitika eest ning tagab selle kooskõla ISMS-i operatiivsete kontrollide ja regulatiivsete nõuetega.

4.1.2 Kinnitab organisatsiooni ajaallikate valiku ja valideerib aja sünkroniseerimise aruandlusprotsessid.

4.2 taristuteenuste juht / võrguinseneeria juht

4.2.1 Haldab organisatsiooni primaarsete ja sekundaarsete NTP-serverite või määratud ajaallikate konfiguratsiooni.

4.2.2 Tagab, et kõik võrku ühendatud seadmed ja virtuaalmasinad sünkroniseerivad aega sobivate intervallidega.

4.2.3 Seirab aja sünkroniseerimise logisid, kellatriivi teavitusi ja tõrkeseisundeid.

[... 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 tuvastatakse ajapõhised ärakasutused või logimise tõrked;

9.1.2 tehakse muudatusi põhilises ajataristus (nt uued organisatsiooni NTP-serverid või protokolliuuendused);

9.1.3 ilmnevad pilveplatvormide kellatriivi lahknevused või piirkondlike teenuste muudatused;

9.1.4 intsidendijärgsed leiud tuvastavad aja ebaühtluse kui kaasaaitava teguri.

9.2 Läbivaatamist koordineerib taristuvaldkonna juht, kaasates vajaduse korral SOC-i, rakendusturbe ja vastavuse sidusrühmad.

9.3 Muudatused tuleb dokumenteerida ISMS-i dokumendiregistris ja edastada mõjutatud sisemistele ning kolmandate osapoolte sidusrühmadele.

9.4 Poliitika varasemad versioonid tuleb turvaliselt arhiveerida, hallata versioonihalduse alusel ja teha need kättesaadavaks vastavus- või õigusauditite taotluste korral.

10. Seotud poliitikad ja seosed

10.1 P1 – Infoturbepoliitika. Sätestab üldise kohustuse tagada kõigi infosüsteemide terviklus ja jälgitavus, mille aluseks on täpne aeg.

10.2 P5 – Muudatuste haldamise poliitika. Reguleerib süsteemikonfiguratsioonide muudatusi, sealhulgas ajaallikate seadistuste muutmist, tagades nõuetekohase dokumenteerimise, testimise ja tagasipööramisplaanid.

10.3 P22 – logimise ja seire poliitika. Sõltub otseselt sünkroniseeritud ajast, et tagada sündmuste järjestus, logide korreleerimine ja intsidendiuurimise terviklus eri süsteemides.

10.4 P30 – Intsidentidele reageerimise poliitika. Tugineb täpsetele ajatempleile digitaalse ekspertiisi uurimistes, intsidendi ajajoone koostamisel ja tõendite valduse ahela tagamisel. Ebatäpne aeg kahjustab intsidendiaruannete usaldusväärsust.

10.5 P20 – lõppseadmete kaitse / pahavara poliitika. Nõuab ajaliselt täpset teavitamist ja käitumuslikku analüüsi, et tuvastada pahavara levik, lateraalne liikumine ja juurdepääsuanomaaliad.

10.6 P6 – Riskijuhtimise poliitika. Määratleb desünkroniseerimise võimaliku operatiivse ja digitaalse ekspertiisi riskina, nõudes mõju maandamiseks käesolevas poliitikas sätestatud kontrollide rakendamist.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – operatiivne planeerimine ja kontroll: nõuab täpsete tehniliste kontrollide, näiteks sünkroniseeritud süsteemikellade, integreerimist usaldusväärseks operatiivseks toimimiseks.

11.2 ISO/IEC 27002:2022 – kontroll 8

11.2.1 Rõhutab kellade täpsust ja nõuab organisatsiooniülest süsteemiaja järjepidevust, et võimaldada logide võrdlemist, uurimist ja tehingute turvalist valideerimist.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – süsteemiaja sünkroniseerimine: nõuab autoriteetsete ajaallikate kasutamist aja sünkroniseerimiseks kõigis süsteemipiiri kuuluvates komponentides.

11.3.2 AU-8 – ajatemplid: tagab sündmuste täpse ajatempliga märgistamise ning jälgitavuse auditi ja intsidendihalduse jaoks.

11.4 EL GDPR (2016/679)

11.4.1 Artikkel 32 – töötlemise turvalisus: kuigi aega ei ole sõnaselgelt nimetatud, nõuab see asjakohaste tehniliste meetmete kasutamist, sealhulgas auditijälgi ja logisid, mille kehtivus ja terviklus sõltuvad olemuslikult sünkroniseeritud ajatemplitest.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(e): nõuab logimise ja tuvastamise võimekust, mis eeldab täpset aja sünkroniseerimist süsteemideüleseks korreleerimiseks ja õigeaegseks reageerimiseks.

11.6 EL DORA (2022/2554)

11.6.1 Artikkel 9 – IKT-riskide juhtimine: nõuab täpset süsteemset telemeetriat riskiseireks ja anomaaliatuvastuseks, mis sõltub täpsest kellade sünkroniseerimisest.

11.6.2 Artikkel 10 – IKT talitluspidevus: nõuab kontrolle, mis tagavad süsteemi tervikluse katkestuste ajal, sealhulgas ajaliselt joondatud sündmuste kirjed.

11.7 COBIT 2019

11.7.1 DSS05.04 – turbesündmuste seire: nõuab ajatemplite terviklust tõhusaks logianalüüsiks ja ohtude tuvastamiseks.

11.7.2 MEA03 – vastavuse seire, hindamine ja auditeerimine: aja sünkroniseerimine toetab täpset vastavusauditit ja aruandlustsükleid.