					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P23S					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	Asjakohased kontrollinõuded
ISO/IEC 27002:2022	Kontroll 8	Süsteemide sünkroniseeritud toimimine
NIST SP 800-53 Rev.5	SC-45, AU-8	Usaldusväärne NTP ja logide ajatemplite täpsus
EL GDPR	Artiklid 5(1)(d), 32	Isikuandmete töötlemise täpsus, vastutus ja terviklus sünkroniseeritud ajatemplite abil
EL NIS2	Artikkel 21(2)(d)	Seire- ja tuvastusvõimekus, mida toetavad sünkroniseeritud logid
EL DORA	Artiklid 10, 15	Talitluspidevus ja täpsed tehnilised kirjed
COBIT 2019	DSS05.02, MEA03	Ajatemplitega sündmused ja tõenduspõhine seire

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud kontrollimeetmed täpse ja sünkroniseeritud aja tagamiseks kõigis süsteemides, mis salvestavad, edastavad või töötlevad organisatsiooni andmeid.

1.2 Aja sünkroniseerimine on hädavajalik, et süsteemilogid oleksid jälgitavad, turbeintsidente saaks korrektselt seostada ning tõendusmaterjal oleks kohtuekspertiisi analüüsi või õigusliku läbivaatamise käigus usaldusväärne.

1.3 Organisatsioon rakendab automaatset aja sünkroniseerimist auditite tervikluse, intsidendihalduse ning ISO 27001, GDPR-i, DORA ja NIS2 nõuete täitmise alusnõudena.

1.4 Käesolev poliitika tagab, et kõik süsteemid kasutavad usaldusväärseid ajaallikaid, käsitsi aja muutmine on välistatud ning kella triiv parandatakse õigeaegselt.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõigile ettevõtte omandis olevatele süsteemidele ja seadmetele, sealhulgas serveritele, lauaarvutitele, sülearvutitele, mobiilseadmetele, tulemüüridele, ruuteritele ja virtuaalmasinatele;

2.1.2 kaug- ja pilvekeskkondades majutatud taristule, mida kasutatakse organisatsiooni tegevuses, sealhulgas AWS-ile, Microsoft 365-le ja SaaS-platvormidele;

2.1.3 süsteemidele, mis loovad või säilitavad sündmuslogisid, autentimiskirjeid või auditijälge;

2.1.4 kõigile töötajatele, töövõtjatele, tarnijatele ja IT-toe teenuseosutajatele, kes vastutavad nende süsteemide seadistamise või haldamise eest.

2.2 Poliitika kohaldub ka isiklikele seadmetele (BYOD), mida kasutatakse ettevõtte süsteemidele juurdepääsuks, kui need seadmed salvestavad või loovad auditi seisukohalt asjakohaseid andmeid.

3. Eesmärgid

3.1 Tagada, et kõik kriitilise tähtsusega süsteemid sünkroniseerivad aja automaatselt usaldusväärsete Network Time Protocoli (NTP) serverite või samaväärsete pilveteenuse pakkuja mehhanismide abil.

3.2 Vältida ajalisi lahknevusi, mis võivad auditite või turbeuurimiste käigus kahjustada süsteemilogide usaldusväärsust või omavahelist seostatavust.

3.3 Võimaldada lubatud lävendeid ületava ajatriivi õigeaegne tuvastamine ja kõrvaldamine.

3.4 Tagada ajatemplite järjepidevus kõigis keskkondades, sealhulgas kohapealses taristus, pilvekeskkondades ja kaugkeskkondades.

3.5 Täita kirjete ja sündmuste tervikluse, jälgitavuse ning ümberlükkamatuse tehnilised ja õiguslikud nõuded.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 kiidab käesoleva poliitika heaks ja tagab organisatsiooni nõuetele vastavuse;

4.1.2 teeb järelevalvet süsteemitaseme aja täpsuse perioodiliste läbivaatamiste ja rakenduslünkade üle;

4.1.3 kiidab põhjendatud ja dokumenteeritud juhtudel heaks automaatse aja sünkroniseerimise erandid.

4.2 IT-toe teenuseosutaja / sisemine IT-vastutaja

4.2.1 seadistab aja sünkroniseerimise kõigis ettevõtte omandis olevates või hallatavates süsteemides;

4.2.2 kontrollib, et igapäevane või muu ajastatud sünkroniseerimine toimib nõuetekohaselt;

4.2.3 uurib ja kõrvaldab ajatriivi juhtumid, sünkroniseerimistõrked ning NTP-teenusele juurdepääsu probleemid;

4.2.4 dokumenteerib aja sünkroniseerimise oleku igakuiste süsteemide tervisekontrollide osana.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Korrapärane läbivaatamine

9.1.1 käesolev poliitika tuleb kord aastas läbi vaadata tegevjuhi, IT-toe teenuseosutaja ja andmekaitsekoordinaatori poolt;

9.1.2 läbivaatamisel tuleb arvesse võtta kõiki logisid ja aja sünkroniseerimise nõuetele vastavuse staatuse aruandeid.

9.2 Sündmuspõhised ajakohastamised

9.2.1 Käesolevat poliitikat tuleb ajakohastada, kui:

9.2.1.1 süsteemitõrge põhjustab olulise ajatriivi;

9.2.1.2 audit tuvastab puudused aja sünkroniseerimises;

9.2.1.3 organisatsioon võtab kasutusele uued pilve-, hübriid- või virtualiseerimiskeskkonnad;

9.2.1.4 õiguslikud või regulatiivsed muudatused kehtestavad uued aja tervikluse nõuded.

9.3 Versioonihaldus ja teavitamine

9.3.1 kõik ajakohastused peavad olema versioonistatud ja kuupäevastatud;

9.3.2 olulistest muudatustest tuleb teavitada kogu tehnilist personali;

9.3.3 varasemaid versioone tuleb auditi toetamiseks säilitada 3 aastat.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat tuleb rakendada koos järgmiste VKE poliitikatega:

10.1.1 P22S – logimis- ja seirepoliitika: tagab logide järjepidevad ajatemplid jälgitavuse ja kohtuekspertiisi seostatavuse jaoks.

10.1.2 P30S – intsidentidele reageerimise poliitika (P30): tugineb ajatemplite täpsusele, et rekonstrueerida intsidente, määratleda ajajooni ja toetada teavitamisotsuseid.

10.1.3 P17S – andmekaitse- ja privaatsuspoliitika: tagab, et isikuandmetega seotud juurdepääsulogid ja andmekäitluse ajajooned on täpsed ning GDPR-i kohaselt kaitstavad.

10.1.4 P12S – varahalduse poliitika: toetab sünkroniseerimist vajavate süsteemide tuvastamist, eelkõige mobiilsete ja kaugseadmete puhul.

10.1.5 P26S – kolmandate osapoolte ja tarnijate turbepoliitika: tagab, et tarnijad, kellel on lepinguline juurdepääs organisatsiooni andmetele või kes neid logivad, järgivad sünkroniseeritud aja kasutamise nõudeid.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab turvaliseks toimimiseks vajalike kontrollimeetmete rakendamist, sealhulgas logimist ja ajatemplite kasutamist.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.17 – soovitab sünkroniseeritud aega kõigile süsteemidele, mis loovad logisid või toimivad koostalitlusvõimeliselt.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-8 – nõuab sisemiste või väliste ajaallikate kasutamist logide ajatemplite täpsuse tagamiseks.

11.3.2 SC-45 – täpsustab usaldusväärsete NTP-allikate kasutamist ning käsitsi aja muutmise vältimist kriitilise tähtsusega süsteemides.

11.4 EL GDPR

11.4.1 Artikkel 5(1)(d) – nõuab isikuandmete töötlemisel täpsust ja vastutust, mida toetavad sünkroniseeritud ajatemplid.

11.4.2 Artikkel 32 – nõuab andmete tervikluse tagavaid turvameetmeid, sealhulgas järjepidevaid logimise ajaraame.

11.5 EL NIS2 direktiiv

11.5.1 Artikkel 21(2)(d) – nõuab seire- ja tuvastusvõimekust, mida toetavad sünkroniseeritud süsteemilogid.

11.6 EL DORA

11.6.1 Artikkel 10 – nõuab talitluspidevust, mille eelduseks on jälgitavad ja ajatemplitega IKT-intsidentide logid.

11.6.2 Artikkel 15 – nõuab teenuseosutajatelt täpsete tehniliste kirjete pidamist, sealhulgas ajatemplitega auditijälge.

11.7 COBIT 2019

11.7.1 DSS05.02 – rõhutab ajatemplite terviklust sündmuste tuvastamisel ja neile reageerimisel.

11.7.2 MEA03.01 – nõuab tõenduspõhist toimivuse seiret, mida toetavad täpsed, ajas sünkroniseeritud andmed.