

				Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P23S				Dokumentum címe: Időszinkronizálási szabályzat							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025		A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Ürlap		Nyilvántartás		Egyéb

Felülvizsgálati előzmények				
Felülvizsgálat száma	Felülvizsgálat dátuma	Változások	Felülvizsgálta	A folyamat tulajdonosa

Jóváhagyások			
Név	Beosztás	Dátum	Aláírás

<p>Jogi nyilatkozat (szerzői jog és felhasználási korlátozások) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.</p> <p>A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után.</p> <p>Licenceléssel kapcsolatban keresse: info@clarysec.com</p>
--

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. pont	Releváns kontrollkövetelmények
ISO/IEC 27002:2022	8. kontroll	Szinkronizált rendszerüzemeltetés
NIST SP 800-53 Rev.5	SC-45, AU-8	Megbízható NTP és a naplói időbélyegek pontossága
GDPR	5. cikk (1) bekezdés d) pont, 32. cikk	Pontosság, elszámoltathatóság és sértetlenség a személyes adatok kezelésében szinkronizált időbélyegek alkalmazásával
NIS2 irányelv	21. cikk (2) bekezdés d) pont	A monitorozási és észlelési képességeket a szinkronizált naplók támogatják
DORA-rendelet	10. cikk, 15. cikk	Operatív reziliencia és pontos műszaki nyilvántartások
COBIT 2019	DSS05.02, MEA03	Időbélyegzett események és bizonyítékokon alapuló monitorozás

1. Cél

1.1 Jelen szabályzat kötelező kontrollokat határoz meg a pontos és szinkronizált idő fenntartására valamennyi olyan rendszerben, amely szervezeti adatokat tárol, továbbít vagy kezel.

1.2 Az időszinkronizálás alapvető fontosságú annak biztosításához, hogy a rendszernaplók visszakövethetők legyenek, a biztonsági incidensek pontosan korrelálhatók legyenek, valamint hogy a bizonyítékok forenzikus elemzés vagy jogi felülvizsgálat során megbízhatóan felhasználhatók legyenek.

1.3 A szervezet az automatizált időszinkronizálást az auditok sértetlensége, az incidenskezelés, valamint az ISO 27001, a GDPR, a DORA és a NIS2 szerinti megfelelés alapvető követelményeként alkalmazza.

1.4 Jelen szabályzat biztosítja, hogy valamennyi rendszer megbízható időforrásokat használjon, megakadályozza az időbeállítások manuális felülírását, és előírja az órák eltérésének időben történő helyesbítését.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi vállalati tulajdonú rendszerre és eszközre, beleértve a szervereket, asztali számítógépeket, laptopokat, mobil eszközöket, tűzfalakat, útválasztókat és virtuális gépeket;

2.1.2 az üzemeltetésben használt távoli és felhőalapú infrastruktúrára (pl. AWS, Microsoft 365, SaaS-platformok);

2.1.3 azokra a rendszerekre, amelyek eseménynaplókat, hitelesítési nyilvántartásokat vagy auditnyomokat hoznak létre vagy tárolnak;

2.1.4 minden olyan munkavállalóra, vállalkozóra, beszállítóra vagy IT-támogatást nyújtó szolgáltatóra, aki e rendszerek konfigurálásáért vagy fenntartásáért felelős.

2.2 A szabályzat kiterjed a BYOD (saját eszköz használata) végpontokra is, amennyiben azokat üzleti rendszerek elérésére használják, és ezek a végpontok auditálás szempontjából releváns adatokat tárolnak vagy hoznak létre.

3. Célkitűzések

3.1 Biztosítani kell, hogy minden kritikus rendszer automatikusan szinkronizálja az időt megbízható Network Time Protocol (NTP) szerverek vagy azokkal egyenértékű felhőszolgáltatói mechanizmusok használatával.

3.2 Meg kell előzni az olyan időeltéréseket, amelyek auditok vagy biztonsági vizsgálatok során alááshatják a rendszernaplók megbízhatóságát vagy korrelálhatóságát.

3.3 Lehetővé kell tenni az elfogadható küszöbértéket meghaladó időeltérés időben történő észlelését és helyesbítését.

3.4 Fenn kell tartani az egységes időbélyegzést minden környezetben (helyszíni, felhőalapú és távoli).

3.5 Teljesíteni kell a nyilvántartások és események sértetlenségére, visszakövethetőségére és letagadhatatlanságára vonatkozó műszaki és jogi követelményeket.

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 Jóváhagyja jelen szabályzatot, és biztosítja a szervezeti megfelelést.

4.1.2 Felügyeli a rendszerszintű időpontosság és a végrehajtási hiányosságok időszakos felülvizsgálatát.

4.1.3 Indokolt és dokumentált esetben jóváhagyja az automatizált időszinkronizálás alóli kivételeket.

4.2 IT-támogatási szolgáltató / belső IT-funkció

4.2.1 Beállítja az időszinkronizálást valamennyi vállalati tulajdonú vagy kezelt rendszer esetében.

4.2.2 Ellenőrzi, hogy a napi vagy ütemezett szinkronizálás megfelelően működik-e.

4.2.3 Kivizsgálja és elhárítja az időeltérési eseményeket, a szinkronizálási hibákat vagy az NTP-hozzáférési problémákat.

4.2.4 A havi rendszerállapot-ellenőrzések részeként dokumentálja az időszinkronizálás állapotát.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1 Ütemezett felülvizsgálat

9.1.1 Jelen szabályzatot az ügyvezetőnek, az IT-támogatási szolgáltatónak és az adatvédelmi koordinátornak évente felül kell vizsgálnia.

9.1.2 A felülvizsgálat során figyelembe kell venni valamennyi naplót és az időszinkronizálási megfelelési állapotjelentéseket.

9.2 Esemény által kiváltott frissítések

9.2.1 Jelen szabályzatot frissíteni kell, ha:

9.2.1.1 egy rendszerhiba jelentős időeltérést eredményez;

9.2.1.2 egy audit hiányosságokat tár fel az időszinkronizálásban;

9.2.1.3 a szervezet új felhőalapú, hibrid vagy virtualizált környezeteket vezet be;

9.2.1.4 jogi vagy szabályozási változások új időintegritási követelményeket vezetnek be.

9.3 Verziókezelés és kommunikáció

9.3.1 Minden frissítést verzióval és dátummal kell ellátni.

9.3.2 A jelentős módosításokat kommunikálni kell valamennyi műszaki munkatárs felé.

9.3.3 Az előző verziókat auditcélből 3 évig meg kell őrizni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi KKV-szabályzatokkal együtt kell alkalmazni:

10.1.1 P22S – Naplózási és felügyeleti szabályzat: Biztosítja a naplók egységes időbélyegzését a visszakövethetőség és a forenzikus korreláció érdekében.

10.1.2 P30S – Incidenskezelési szabályzat: Az incidensek rekonstruálásához, az idővonalak meghatározásához és az értesítési döntések támogatásához pontos időbélyegekre támaszkodik.

10.1.3 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Biztosítja, hogy a személyes adatokat érintő hozzáférési naplók és adatkezelési idővonalak pontosak legyenek, és a GDPR alapján igazolhatók maradjanak.

10.1.4 P12S – Eszközkezelési szabályzat: Támogatja a szinkronizálást igénylő rendszerek azonosítását, különösen a mobil és távoli eszközök esetében.

10.1.5 P26S – Harmadik felek és beszállítói biztonsági szabályzat: Biztosítja, hogy azok a beszállítók, amelyek a szervezet számára adatokat érnek el vagy naplóznak, szerződéses alapon szinkronizált időkezelési gyakorlatot alkalmazzanak.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:

11.1.1 8.1 pont – Előírja a biztonságos működéshez szükséges kontrollok bevezetését, beleértve a naplózást és az időbélyegzést.

11.2 ISO/IEC 27002:

11.2.1 8.17 kontroll – Szinkronizált idő alkalmazását javasolja minden olyan rendszer esetében, amely naplókat hoz létre vagy együttműködő módon működik.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Előírja belső vagy külső időforrások használatát a naplók időbélyegeinek pontossága érdekében.

11.3.2 SC-45 – Meghatározza a megbízható NTP-források használatát és a manuális időmódosítás megakadályozását a kritikus rendszerekben.

11.4 GDPR:

11.4.1 5. cikk (1) bekezdés d) pont – Előírja a személyes adatok kezelésének pontosságát és elszámoltathatóságát, amelyet a szinkronizált időbélyegek támogatnak.

11.4.2 32. cikk – Előírja az adatintegritást biztosító biztonsági intézkedéseket, amelyek körébe a következetes naplózási időkeretek is beletartoznak.

11.5 NIS2 irányelv:

11.5.1 21. cikk (2) bekezdés d) pont – Előírja a monitorozási és észlelési képességeket, amelyeket a szinkronizált rendszernaplók támogatnak.

11.6 DORA-rendelet:

11.6.1 10. cikk – Operatív rezilienciát követel meg, amelyhez visszakövethető és időbélyegzett IKT-incidensnaplók szükségesek.

11.6.2 15. cikk – Előírja, hogy a szolgáltatók pontos műszaki nyilvántartásokat vezessenek, beleértve az időbélyegzett auditnyomokat is.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Hangsúlyozza az időbélyegek sértetlenségének fontosságát az események észlelése és a reagálás szempontjából.

11.7.2 MEA03.01 – Bizonyítékokon alapuló teljesítmény-monitorozást ír elő, amelyet pontos, idősinkronizált adatok támogatnak.