

				Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P23				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	-
ISO/IEC 27002:2022	8. kontroll	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
GDPR	32. cikk	-
NIS2 irányelv	21. cikk (2) bekezdés e) pont	-
DORA-rendelet	9., 10. cikk	-
COBIT 2019	DSS05.04, MEA	-

1. Cél

1.1 Jelen szabályzat célja annak biztosítása, hogy a szervezet valamennyi rendszere, alkalmazása, eszköze és felhőszolgáltatása egységes és pontos időbeállításokat tartson fenn a kijelölt, megbízható időforrásokkal történő szinkronizálás révén.

1.2 A pontos időszinkronizálás alapvető fontosságú a megbízható naplózáshoz, a biztonságos kommunikációhoz, az auditnyomok visszakövethetőségéhez, az incidenskezeléshez és a forenzikus vizsgálatokhoz. Az eltérő időbeállítások nem összevethető naplókat, sikertelen hitelesítést és hiányos, előírt jelentéstételt eredményezhetnek.

1.3 Ez a szabályzat azáltal támogatja az ISO/IEC 27001 A mellékletének 8.17. kontrollját és a kapcsolódó nemzetközi szabványokat, hogy előírja az időpontosság biztosítását és az óraelterések észlelését a szervezet teljes IT-környezetében.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi infrastruktúra-összetevőre, beleértve a szervereket, munkaállomásokat, hálózati eszközöket, tűzfalakat és IoT-rendszereket;

2.1.2 virtuális és felhőkörnyezetekre (pl. AWS, Azure, Google Cloud);

2.1.3 minden olyan rendszerre, amely naplózásban, hitelesítésben, tranzakciófeldolgozásban vagy biztonsági események korrelációjában vesz részt;

2.1.4 a belső munkavállalókra, vállalkozókra és harmadik fél szolgáltatókra, akik időérzékeny rendszerekért felelősek.

2.2 A hatály kiterjed minden olyan rendszerre is, amely időbélyeggel ellátott nyilvántartásokat hoz létre vagy használ fel, például naplóbejegyzéseket, riasztásokat, felhasználói tevékenységnaplókat vagy forenzikus bizonyítékokat.

3. Célkitűzések

3.1 Jóváhagyott NTP-forrásokra vagy azzal egyenértékű megoldásra épülő, egységes, központi időszinkronizálási architektúra meghatározása.

3.2 Annak biztosítása, hogy valamennyi rendszer meghatározott időközönként szinkronizálja az óráját, és hogy az eltérések automatikusan vagy minimális beavatkozással észlelhetők és helyesbíthetők legyenek.

3.3 Az órák pontosságának fenntartása hibrid, helyszíni és felhőalapú környezetekben annak érdekében, hogy biztosított legyen:

3.3.1 a megbízható eseménykorreláció és az incidenskezelés;

3.3.2 az olyan szabványoknak és jogszabályoknak való megfelelés, mint az ISO 27001, a GDPR, a NIS2 és a DORA;

3.3.3 a visszajátszásos támadásokkal és az időalapú hitelesítési hibákkal szembeni védelem.

3.4 Egyértelmű szerepkörök, kivételkezelési eljárások és auditmechanizmusok kialakítása a szabályzat betartásának fenntartása érdekében.

3.5 Annak biztosítása, hogy az idővel kapcsolatos rendellenességek naplózásra kerüljenek, riasztást váltsanak ki, és a tűréshatárok túllépése esetén eszkaláció történjen.

4. Szerepkörök és felelősségi körök

4.1 Információbiztonsági vezető

4.1.1 A szabályzat gazdája, és biztosítja annak összhangját az információbiztonság-irányítási rendszer (ISMS) működési kontrolljaival és a jogszabályi követelményekkel.

4.1.2 Jóváhagyja a szervezeti időforrások kiválasztását, és felügyeli az időszinkronizálással kapcsolatos jelentéstételi folyamatokat.

4.2 Infrastruktúra-szolgáltatási vezető / hálózatüzemeltetési vezető

4.2.1 Fenntartja a szervezet elsődleges és másodlagos NTP-szervereit, illetve a kijelölt időforrás-konfigurációt.

4.2.2 Biztosítja, hogy valamennyi hálózatba kapcsolt eszköz és virtuális példány megfelelő időközönként szinkronizálja az időt.

4.2.3 Nyomon követi az időszinkronizálási naplókat, az óraeltérési riasztásokat és a hibaállapotokat.

[... 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 Jelen szabályzatot évente, vagy az alábbi feltételek bármelyikének fennállása esetén ennél korábban felül kell vizsgálni:

9.1.1 időalapú exploitok vagy naplózási hibák észlelése;

9.1.2 a központi időinfrastruktúrát érintő változások (pl. új vállalati NTP-szerverek vagy protokollfrissítések);

9.1.3 felhőplatformok időeltérési anomáliái vagy regionális szolgáltatásváltozások;

9.1.4 olyan incidens utáni megállapítások, amelyek szerint az időeltérés hozzájáruló tényező volt.

9.2 A felülvizsgálatot az infrastruktúra-terület vezetője koordinálja, a SOC, az alkalmazásbiztonsági és a megfelelőségi érintettek szükséges közreműködésével.

9.3 A módosításokat az ISMS dokumentumnyilvántartásában kell dokumentálni, és azokról az érintett belső és külső feleket tájékoztatni kell.

9.4 A szabályzat korábbi verzióit biztonságosan archiválni kell, verziókezelés alatt kell tartani, és hozzáférhetővé kell tenni megfelelőségi vagy jogi auditkéresek esetén.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 – Információbiztonsági szabályzat. Meghatározza az összes információs rendszer sértetlenségének és visszakövethetőségének biztosítására vonatkozó átfogó elvárást, amelynek alapfeltétele a pontos időkezelés.

10.2 P5 – Változáskezelési szabályzat. Szabályozza a rendszerkonfigurációk módosításait, beleértve az időforrások beállításainak változtatását is, biztosítva a megfelelő dokumentálást, tesztelést és a visszaállítási tervet.

10.3 P22 – Naplózási és felügyeleti szabályzat. Közvetlenül függ a szinkronizált időtől annak biztosítása érdekében, hogy a különböző rendszerekben az eseménysorrend, a naplókorreláció és az incidenskivizsgálás sértetlensége fenntartható legyen.

10.4 P30 – Incidenskezelési szabályzat. A forenzikus vizsgálatok, az incidens-idővonalak és a bizonyítéklánc-dokumentáció szempontjából pontos időbélyegekre támaszkodik. A pontatlan idő aláássa az incidensjelentések hitelességét.

10.5 P20 – Végpontvédelemi / kártevővédelmi szabályzat. Előírja az időben pontos riasztást és a viselkedésalapú elemzést a kártevők terjedésének, az oldalirányú mozgásnak és a hozzáférési rendellenességeknek az észleléséhez.

10.6 P6 – Kockázatkezelési szabályzat. Az időszinkronizáció hiányát potenciális működési és forenzikus kockázatként kezeli, amelynek csökkentésére a jelen szabályzatban meghatározott kontrollokat kell alkalmazni.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont – Operatív tervezés és felügyelet: előírja olyan pontos technikai kontrollok integrálását, mint a szinkronizált rendszerórák, a megbízható operatív végrehajtás érdekében.

11.2 ISO/IEC 27002:2022 – 8. kontroll

11.2.1 Megerősíti az órák pontosságának követelményét, és előírja a rendszeridő szervezeti szintű egységességét a naplók összehasonlíthatósága, a kivizsgálás és a biztonságos tranzakcióellenőrzés elősegítése érdekében.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Rendszeridő szinkronizálása: előírja az időszinkronizálást hiteles források használatával a rendszerhatáron belüli valamennyi összetevő esetében.

11.3.2 AU-8 – Időbélyegek: biztosítja, hogy az események pontos időbélyeggel legyenek ellátva, és visszakövethetőséget nyújtsanak az audit és az incidenskezelés számára.

11.4 GDPR (2016/679)

11.4.1 32. cikk – Az adatkezelés biztonsága: bár kifejezetten nem nevesíti az időt, előírja a megfelelő technikai intézkedések — beleértve az auditnyomokat és naplókat — alkalmazását, amelyek érvényessége és sértetlensége eredendően a szinkronizált időbélyegektől függ.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés e) pont: előírja a naplózási és észlelési képességeket, amelyek feltételezik a pontos időszinkronizálást a rendszerek közötti korreláció és az időben történő reagálás érdekében.

11.6 DORA-rendelet (2022/2554)

11.6.1 9. cikk – IKT-kockázatkezelés: előírja a pontos rendszertelemetria biztosítását a kockázatok nyomon követéséhez és az anomáliák észleléséhez, ami a rendszerórák precíz szinkronizálásától függ.

11.6.2 10. cikk – IKT-üzletmenet-folytonosság: olyan kontrollok alkalmazását írja elő, amelyek a zavarok idején is biztosítják a rendszerek sértetlenségét, beleértve az időben összehangolt eseménnyilvántartásokat is.

11.7 COBIT 2019

11.7.1 DSS05.04 – Biztonsági események megfigyelése: előírja az időbélyegek sértetlenségét a hatékony naplóelemzés és fenyegetésészlelés érdekében.

11.7.2 MEA03 – A megfelelés nyomon követése, értékelése és felmérése: az időszinkronizálás támogatja a pontos megfelelési auditálást és jelentéstételi ciklusokat.

