					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P23					Заглавие на документа: **Политика за синхронизация на времето**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Clause 8	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
EU GDPR	Article 32	-
EU NIS2	Article 21(2)(e)	-
EU DORA	Articles 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Цел

1.1 Целта на тази политика е да гарантира, че всички системи, приложения, устройства и облачни услуги в организацията поддържат последователни и точни настройки на времето чрез синхронизация с определени доверени източници на време.

1.2 Точната синхронизация на времето е от съществено значение за надеждното регистриране, защитените комуникации, одитната следа, реагирането при инциденти и форензичните разследвания. Несъответствията във времето могат да доведат до некорелирани журнали, неуспешна автентикация и непълно регулаторно докладване.

1.3 Тази политика подпомага контрол 8.17 от Приложение А на ISO/IEC 27001 и свързаните международни стандарти, като налага точност на времето и откриване на отклонения на системния часовник в цялата ИТ среда на организацията.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 Всички компоненти на инфраструктурата, включително сървъри, работни станции, мрежови устройства, защитни стени и системи за Интернет на нещата (IoT)

2.1.2 Виртуални и облачни среди (напр. AWS, Azure, Google Cloud)

2.1.3 Всички системи, участващи в регистриране, автентикация, обработка на транзакции или корелация на събития по сигурността

2.1.4 Вътрешни служители, външни изпълнители и външни доставчици на услуги, които отговарят за системи, чувствителни към времето

2.2 Системите, които генерират или използват записи с времеви маркер — като записи в журнали, предупреждения, записи за потребителска дейност или форензични доказателства — се считат за включени в обхвата.

3. Цели

3.1 Да се дефинира последователна, централизирана архитектура за синхронизация на времето чрез използване на одобрени източници по Network Time Protocol (NTP) или еквивалентни механизми.

3.2 Да се гарантира, че всички системи синхронизират системните си часовници на определени интервали и че всяко отклонение на времето се открива и коригира автоматично или с минимална намеса.

3.3 Да се поддържа точност на времето в хибридни, локални и облачни среди, за да се осигури:

3.3.1 Надеждна корелация на събитията и ефективно реагиране при инциденти

3.3.2 Регулаторно съответствие със стандарти като ISO 27001, GDPR, NIS2 и DORA

3.3.3 Защита срещу replay атаки и откази при автентикация, базирани на време

3.4 Да се установят ясни роли, процедури за обработка на изключения и механизми за одит с цел поддържане на прилагането на политиката.

3.5 Да се гарантира, че аномалиите, свързани с времето, се регистрират, по тях се генерират предупреждения и се ескалират при превишаване на допустимите отклонения.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за тази политика и гарантира съгласуваността ѝ с оперативните контроли на Системата за управление на информационната сигурност (СУИС) и с регулаторните изисквания.

4.1.2 Одобрява избора на корпоративни източници на време и валидира процесите за докладване на синхронизацията на времето.

4.2 Мениджър „Инфраструктурни услуги“ / Ръководител „Мрежово инженерство“

4.2.1 Поддържа основните и резервните NTP сървъри на организацията или определената конфигурация на източниците на време.

4.2.2 Гарантира, че всички мрежово свързани устройства и виртуални инстанции синхронизират времето на подходящи интервали.

4.2.3 Наблюдава журналите за синхронизация на времето, предупрежденията за отклонение на системния часовник и състоянията на отказ.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Преглед и актуализация на изискванията

9.1 Тази политика трябва да се преглежда ежегодно или по-рано при следните условия:

9.1.1 Установяване на експлойти, базирани на време, или откази при регистрирането

9.1.2 Промени в основната инфраструктура за време (напр. нови корпоративни NTP сървъри или актуализации на протоколи)

9.1.3 Несъответствия в отклонението на времето в облачни платформи или промени в регионални услуги

9.1.4 Констатации след инцидент, които идентифицират несъответствие на времето като допринасящ фактор

9.2 Прегледът трябва да бъде координиран от ръководителя на инфраструктурата с необходимия принос от SOC, сигурността на приложенията и заинтересованите страни по съответствието.

9.3 Всички промени трябва да бъдат документирани в Регистъра на документите на СУИС и комуникирани до засегнатите вътрешни заинтересовани страни и трети страни.

9.4 Историческите версии на политиката трябва да бъдат сигурно архивирани, с управление на версиите, и предоставяни при поискване за целите на съответствието или правен одит.

10. Свързани политики и връзки

10.1 P1 – Политика за информационна сигурност. Установява общото изискване за гарантиране на целостта и проследимостта на всички информационни системи, за което точността на времето е основополагаща.

10.2 P5 – Политика за управление на промените. Регламентира промените в системните конфигурации, включително промените в източниците на време, като гарантира надлежно документиране, тестване и планове за отмяна.

10.3 P22 – Политика за регистриране и мониторинг. Пряко зависи от синхронизираното време, за да осигури последователност на събитията, корелация на журнали и цялост на разследванията на инциденти в различни системи.

10.4 P30 – Политика за реагиране при инциденти. Разчита на точни времеви маркери за форензични разследвания, хронология на инцидентите и документация за веригата на съхранение. Неточното време подкопава достоверността на докладите за инциденти.

10.5 P20 – Политика за защита на крайните точки / зловреден софтуер. Изисква предупреждения с точна времева привързаност и поведенчески анализ за откриване на разпространение на зловреден софтуер, странично придвижване и аномалии в достъпа.

10.6 P6 – Политика за управление на риска. Определя десинхронизацията като потенциален оперативен и форензичен риск и изисква контролите, определени в тази политика, за смекчаване на въздействието.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Оперативно планиране и контрол: Изисква интегриране на точни технически контроли, като синхронизирани системни часовници, за надеждно изпълнение на операциите.

11.2 ISO/IEC 27002:2022 – Контрол 8

11.2.1 Подчертава точността на часовника и изисква организационна последователност на системното време с цел улесняване на сравняването на журнали, разследванията и валидирането на защитени транзакции.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Синхронизация на системното време: Изисква синхронизация на времето чрез официални източници за всички компоненти в границите на системата.

11.3.2 AU-8 – Времеви маркери: Осигурява точно времево маркиране на събитията и гарантира проследимост за одит и реагиране при инциденти.

11.4 EU GDPR (2016/679)

11.4.1 Член 32 – Сигурност на обработването: Макар да не посочва изрично времето, изисква използването на подходящи технически мерки — включително одитна следа и журнали — които по своята същност зависят от синхронизирани времеви маркери за валидност и цялост.

11.5 Директива EU NIS2 (2022/2555)

11.5.1 Член 21(2)(e): Изисква възможности за регистриране и откриване, които предполагат точна синхронизация на времето за междусистемна корелация и навременна реакция.

11.6 EU DORA (2022/2554)

11.6.1 Член 9 – Управление на ИКТ риска: Изисква точна системна телеметрия за мониторинг на риска и откриване на аномалии, което зависи от прецизна синхронизация на часовниците.

11.6.2 Член 10 – Непрекъсваемост на ИКТ услугите: Налага контроли, гарантиращи целостта на системите при прекъсвания, включително записи на събития, съгласувани по време.

11.7 COBIT 2019

11.7.1 DSS05.04 – Наблюдение на събития по сигурността: Изисква цялост на времевите маркери за ефективен анализ на журнали и откриване на заплахи.

11.7.2 MEA03 – Мониторинг, оценяване и преценка на съответствието: Синхронизацията на времето подпомага точния одит на съответствието и циклите на докладване.