					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P23S					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	Клауза 8	Относими изисквания към контролите
ISO/IEC 27002:2022	Контрол 8	Синхронизирана работа на системите
NIST SP 800-53 Rev.5	SC-45, AU-8	Доверени NTP източници и точност на времевите маркери в журналите
GDPR на ЕС	Членове 5(1)(d), 32	Точност, отчетност и цялостност при обработването на лични данни чрез синхронизирани времеви маркери
Директива NIS2 на ЕС	Член 21(2)(d)	Възможности за мониторинг и откриване, подпомогнати от синхронизирани журнали
DORA на ЕС	Членове 10, 15	Оперативна устойчивост и точни технически записи
COBIT 2019	DSS05.02, MEA03	Събития с времеви маркери и мониторинг, основан на доказателства

1. Цел

1.1 Настоящата политика установява задължителни контроли за поддържане на точно и синхронизирано време във всички системи, които съхраняват, предават или обработват данни на организацията.

1.2 Синхронизацията на времето е от съществено значение, за да се гарантира, че системните журнали са проследими, инцидентите по сигурността се корелират точно и на доказателствата може да се разчита при форензичен анализ или правен преглед.

1.3 Организацията прилага автоматизирана синхронизация на времето като основно изискване за цялостността на одитната следа, реагирането при инциденти и регулаторното съответствие по ISO 27001, GDPR, DORA и NIS2.

1.4 Настоящата политика гарантира, че всички системи използват доверени източници на време, предотвратява ръчното пренастройване на времето и изисква своевременно коригиране на отклоненията на системния часовник.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички системи и устройства, притежавани от компанията, включително сървъри, настолни компютри, преносими компютри, мобилни устройства, защитни стени, маршрутизатори и виртуални машини

2.1.2 Отдалечена и облачно хоствана инфраструктура, използвана в дейността (напр. AWS, Microsoft 365, SaaS платформи)

2.1.3 Системи, които генерират или съхраняват журнали за събития, записи за автентикация или одитна следа

2.1.4 Всеки служител, външен изпълнител, доставчик или доставчик на ИТ поддръжка, отговорен за конфигурирането или поддръжката на тези системи

2.2 Политиката се прилага и за BYOD крайни точки (използване на лични устройства), използвани за достъп до служебни системи, при условие че тези крайни точки съхраняват или генерират данни, имащи значение за одита.

3. Цели

3.1 Да се гарантира, че всички критични системи автоматично синхронизират времето си чрез доверени сървъри по Network Time Protocol (NTP) или еквивалентни механизми на облачния доставчик

3.2 Да се предотвратят разлики във времето, които биха могли да подкопаят надеждността или корелацията на системните журнали по време на одити или разследвания по сигурността

3.3 Да се осигури своевременно откриване и коригиране на отклонения във времето извън допустимите прагове

3.4 Да се поддържа последователно времево маркиране във всички среди (локални, облачни и отдалечени)

3.5 Да се изпълнят техническите и правните изисквания за цялостност, проследимост и неотричане на записи и събития

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява настоящата политика и гарантира организационно съответствие

4.1.2 Осъществява надзор върху периодичните прегледи на точността на времето на системно ниво и установените пропуски при внедряването

4.1.3 Одобрява изключения от автоматизираната синхронизация на времето, когато са обосновани и документирани

4.2 Доставчик на ИТ поддръжка / вътрешна ИТ функция

4.2.1 Конфигурира синхронизацията на времето за всички системи, притежавани или управлявани от компанията

4.2.2 Проверява ежедневно или по график дали синхронизацията функционира коректно

4.2.3 Разследва и отстранява отклонения във времето, неуспехи при синхронизацията или проблеми с достъпа до NTP

4.2.4 Документира състоянието на синхронизацията на времето като част от месечните проверки на техническото състояние на системите

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

9. Изисквания за преглед и актуализация

9.1 Планиран преглед

9.1.1 Настоящата политика трябва да се преглежда ежегодно от Управителя, доставчика на ИТ поддръжка и Координатора по поверителността

9.1.2 При прегледа трябва да се вземат предвид всички журнали и отчетите за статуса на съответствието относно синхронизацията на времето

9.2 Актуализации, задействани от събития

9.2.1 Настоящата политика трябва да бъде актуализирана, ако:

9.2.1.1 Системен отказ доведе до значително отклонение на времето

9.2.1.2 Одит разкрие дефицити в синхронизацията на времето

9.2.1.3 Организацията въведе нови облачни, хибридни или виртуализирани среди

9.2.1.4 Правни или регулаторни промени въведат нови изисквания за цялостност на времето

9.3 Управление на версиите и комуникация

9.3.1 Всички актуализации трябва да бъдат версионирани и датирани

9.3.2 Съществени промени трябва да бъдат комуникирани до целия технически персонал

9.3.3 Предходните версии трябва да се съхраняват 3 години в подкрепа на одита

10. Свързани политики и връзки

10.1 Настоящата политика трябва да се прилага съвместно със следните SME политики:

10.1.1 P22S – Политика за регистриране и мониторинг: Осигурява последователно времево маркиране в журналите за проследимост и форензична корелация.

10.1.2 P30S – Политика за реагиране при инциденти: Разчита на точността на времевите маркери за възстановяване на хронологията на инцидентите, определяне на времеви линии и подпомагане на решенията за уведомяване.

10.1.3 P17S – Политика за защита на данните и поверителност: Осигурява, че журналите за достъп и времевите линии за обработване на данни, свързани с лични данни, са точни и защитими съгласно GDPR.

10.1.4 P12S – Политика за управление на активите: Подпомага идентифицирането на системите, които изискват синхронизация, особено мобилните и отдалечените устройства.

10.1.5 P26S – Политика за сигурност на трети страни и доставчици: Осигурява, че доставчиците, които осъществяват достъп до данни на организацията или ги регистрират, договорно спазват практики за синхронизирано време.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:

11.1.1 Клауза 8.1 – Изисква внедряване на контроли, необходими за сигурни операции, включително регистриране и времево маркиране.

11.2 ISO/IEC 27002:

11.2.1 Контрол 8.17 – Препоръчва синхронизирано време за всички системи, които създават журнали или работят съвместно.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Изисква използването на вътрешни или външни източници на време за точност на времевите маркери в журналите.

11.3.2 SC-45 – Определя използването на доверени NTP източници и предотвратяването на ръчни промени на времето в критични системи.

11.4 GDPR на ЕС:

11.4.1 Член 5(1)(d) – Изисква точност и отчетност при обработването на лични данни, подпомогнати от синхронизирани времеви маркери.

11.4.2 Член 32 – Изисква мерки за сигурност, гарантиращи цялостност на данните, включително последователни времеви рамки при регистрирането.

11.5 Директива NIS2 на ЕС:

11.5.1 Член 21(2)(d) – Изисква възможности за мониторинг и откриване, подпомогнати от синхронизирани системни журнали.

11.6 DORA на ЕС:

11.6.1 Член 10 – Изисква оперативна устойчивост, налагаща проследими и времево маркирани журнали за ИКТ инциденти.

11.6.2 Член 15 – Изисква доставчиците на услуги да поддържат точни технически записи, включително одитна следа с времеви маркери.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Подчертава цялостността на времевите маркери за откриване и реагиране при събития.

11.7.2 MEA03.01 – Изисква мониторинг на резултатността, основан на доказателства, подпомогнат от точни данни със синхронизирано време.