					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P22					Заглавие на документа: **Политика за регистриране и мониторинг**							
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**

1. Цел

1.1 Целта на тази политика е да установи ясни и задължителни изисквания за генериране, защита, преглед и анализ на журнали, отразяващи ключови системни събития и инциденти по сигурността в ИТ средата на организацията.

1.2 Регистрирането и мониторингът са от критично значение за откриване на аномалии, реагиране при заплахи, форензични разследвания, готовност за одит и регулаторно съответствие. Тази политика гарантира, че всички автоматично генерирани от системите събития се записват, съхраняват и корелират точно чрез синхронизация на времето.

1.3 Тази политика е съществена за подпомагане на ISO/IEC 27001, клауза 8.1, и контролите от приложение A 8.15 (регистриране), 8.16 (мониторинг) и 8.17 (синхронизация на часовниците), и е пряко съотнесена към регулаторните задължения по GDPR, NIS2, DORA и COBIT 2019.

2. Обхват

2.1 Тази политика се прилага за всички системи, услуги и среди, които съхраняват, обработват или пренасят данни, включени в обхвата на Системата за управление на информационната сигурност (СУИС), включително:

2.1.1 локална инфраструктура, облачни услуги (напр. IaaS, PaaS, SaaS) и хибридни среди

2.1.2 операционни системи, бази данни, приложения и мрежови устройства

2.1.3 системи за сигурност като SIEM, защитни стени, платформи за откриване и реагиране на крайни точки (EDR), VPN концентратори и доставчици на идентичност

2.2 Следните заинтересовани страни са в обхвата:

2.2.1 вътрешни потребители със системни или административни привилегии

2.2.2 персонал по ИТ инфраструктура и ИТ операции

2.2.3 Центърът за операции по сигурността (SOC) и екипите по откриване на заплахи

2.2.4 софтуерни разработчици и собственици на приложения

2.2.5 външни доставчици на услуги, които управляват системи, генериращи журнали

3. Цели

3.1 Да се гарантира, че всички критични системи генерират журнали за инциденти по сигурността и записи за системна дейност, които се съхраняват в съответствие с регулаторните, правните и договорните изисквания.

3.2 Да се определят минималните типове събития и съдържанието на журналите, необходими за откриване на неоторизирани дейности, проследяване на действията на потребителите и подпомагане на форензични разследвания.

3.3 Да се прилагат мерки за защита за предотвратяване на подправяне на журнали, неоторизирано изтриване или неконтролиран достъп до данни от журнали.

3.4 Да се внедрят централизирани системи за регистриране и предупреждение (напр. SIEM) за агрегиране, корелация и ескалация на подозрителна активност в близко до реалното време.

3.5 Да се гарантира синхронизация на системните часовници, за да се осигури точна корелация между системите и анализ на инциденти.

3.6 Да се подпомогне непрекъснатото подобрение и съответствието чрез интегриране на мониторинга на журнали с процесите по одит, управление на риска и управление на инциденти.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за тази политика и гарантира, че тя е съобразена с рисковия профил на организацията, изискванията за одит и задълженията по СУИС.

4.1.2 Одобрява обхвата на регистрирането за регулирани системи или системи с висок риск и осъществява надзор върху докладването за съответствие.

4.2 Ръководител на Центъра за операции по сигурността (SOC)

4.2.1 Експлоатира и поддържа централизирани платформи за управление на журнали (напр. SIEM).

4.2.2 Определя правила за агрегиране на журнали, прагове за предупреждения и процедури за ескалация при триаж на инциденти.

4.2.3 Преглежда ежедневните отчети и гарантира, че аномалиите се анализират, документират и ескалират при необходимост.

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

9. Преглед и актуализиране

9.1 Тази политика трябва да се преглежда ежегодно или по-рано в отговор на:

9.1.1 съществени промени в системната архитектура или инфраструктурата за регистриране (напр. миграция на SIEM)

9.1.2 промени в регулаторните изисквания за регистриране (напр. задължения за регистриране по NIS2, DORA)

9.1.3 констатации от одити или прегледи след инцидент

9.1.4 нововъзникващи заплахи, изискващи засилен мониторинг (напр. вътрешни заплахи, компрометиране на веригата на доставки)

9.2 Процесът по преглед следва да се ръководи от Ръководителя на Центъра за операции по сигурността (SOC) в координация с CISO, екипите по управление на риска, съответствие и ИТ инфраструктура.

9.3 Одобрените промени трябва да бъдат под управление на версии в Регистъра за контрол на документи на СУИС и съобщени на:

9.3.1 всички заинтересовани страни с отговорност за поддръжката на системите за регистриране

9.3.2 собствениците на приложения и системи

9.3.3 външни доставчици с отговорности по телеметрия или интеграция със SIEM

9.4 Всички заменени версии трябва да бъдат архивирани по сигурен начин, като достъпът се ограничава до упълномощени отговорници по СУИС за целите на одит и правни производства.

10. Свързани политики и връзки

10.1 P1 – Политика за информационна сигурност. Определя основния ангажимент за защита на системите и данните, в рамките на който регистрирането и мониторингът функционират като ключови детективски контроли и механизми за реагиране.

10.2 P4 – Политика за контрол на достъпа. Гарантира, че привилегированият достъп, потребителските влизания и събитията по оторизация се регистрират в журнали и се наблюдават за злоупотреба или аномално поведение.

10.3 P5 – Политика за управление на промените. Изисква регистриране на системни промени, внедряване на корекции и актуализации на конфигурацията, които могат да въведат риск или неоторизирани изменения.

10.4 P21 – Политика за мрежова сигурност. Изисква регистриране на мрежово ниво (напр. журнали от защитни стени, предупреждения от IDS/IPS, VPN активност) и интеграция със SIEM за видимост върху аномалии в трафика и защита на периметъра.

10.5 P23 – Политика за синхронизация на времето. Налага съгласуваност на часовниците в системите, което е съществено за надеждно регистриране и корелация на събития по сигурността в множество среди.

10.6 P30 – Политика за реагиране при инциденти. Разчита на данни от журнали и механизми за предупреждение за идентифициране, разследване и реагиране при инциденти по сигурността, като същевременно съхранява форензични артефакти за преглед след инцидент.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 8.1 – Планиране и оперативен контрол: Изисква контроли за наблюдение на операциите и защита срещу неоторизиран достъп и неправомерно използване на системите.

11.2 ISO/IEC 27002:2022 – Контроли 8.15, 8.16, 8.17

11.2.1 Определя подробни изисквания за регистриране, включително кои събития трябва да се записват, как да се защитават и анализират журналите и как да се гарантира надеждността на времевите маркери в различните системи.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 до AU-12: Обхваща избора на събития, регистрирането, защитата, одитния преглед, реагирането при откази в одитното регистриране и съхранението на одитни записи.

11.3.2 SI-4 – Наблюдение на системите: Изисква активно наблюдение на системите с предупреждения, базирани на аномална активност.

11.3.3 SC-45 – Синхронизация на системното време: Подсилва изискването за точност на времето с цел проследимост на събитията и корелация на инциденти.

11.4 EU GDPR (2016/679)

11.4.1 Член 32 – Сигурност на обработването: Изисква технически контроли като регистриране и мониторинг за осигуряване на сигурност и отчетност, по-специално по отношение на достъпа до лични данни.

11.5 Директива (ЕС) NIS2 (2022/2555)

11.5.1 Член 21(2)(e): Изисква системи за регистриране на събития и мониторинг за бързо откриване и реагиране при инциденти по сигурността.

11.6 EU DORA (2022/2554)

11.6.1 Член 9 – Управление на ИКТ риска: Изисква механизми за откриване на аномална активност, регистриране на инциденти и съхранение на форензични данни.

11.6.2 Член 11 – Тестване на планове за непрекъсваемост на дейността в областта на ИКТ: Подчертава непрекъсваемостта на мониторинга и валидирането на наличността на журнали по време на оперативни прекъсвания.

11.7 COBIT 2019

11.7.1 DSS01.05 – Управление на журналите за сигурност: Изисква внедряване на възможности за регистриране за цялата критична инфраструктура.

11.7.2 DSS05.04 – Мониторинг на събития по сигурността: Изисква наблюдение и анализ на журнали в реално време за откриване на събития и реагиране.

11.7.3 MEA03 – Мониторинг, оценяване и преценка на съответствието: Изисква редовен преглед на практиките за регистриране и съгласуването им с целите на контролите.