					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P31					Заглавие на документа: **Политика за събиране на одиторски доказателства и форензика**							
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	
ISO/IEC 27002:2022	Контроли 5.25–5.27, 8	
ISO/IEC 27035:2016	Части 1 и 3	
NIST SP 800-53 Rev. 5	IR-1 до IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Форензика на мобилни устройства и носители	Форензика на мобилни устройства и носители
NIST SP 800-86	Интегриране на форензични техники	Интегриране на форензични техники в реагирането при инциденти
GDPR на ЕС	Член 5, 33–34	
NIS2 на ЕС	Член 23(1)–(4)	
DORA на ЕС	Член 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Цел

1.1 Настоящата политика установява структуриран и правно обоснован подход за идентифициране, събиране, запазване, анализ и унищожаване на цифрови доказателства при действителни или предполагаеми инциденти по сигурността.

1.2 Тя гарантира, че процесите за форензична готовност и обработване на доказателства:

1.2.1 поддържат целостта на доказателствата и документацията по веригата на съхранение

1.2.2 подпомагат вътрешни разследвания, съдебни производства или регулаторно докладване

1.2.3 са съгласувани с международно признати форензични стандарти и критерии за допустимост на доказателства

1.3 Политиката подкрепя ангажимента на организацията за проактивно реагиране при инциденти, правно съответствие и прозрачност на управлението, като същевременно свежда до минимум оперативните прекъсвания.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 всички служители, външни изпълнители, доставчици и доставчици на услуги, ангажирани със системно администриране, обработване на инциденти или разследващи дейности

2.1.2 всички крайни устройства, сървъри, приложения, мрежи и облачни платформи под контрола на организацията или в рамките на договорната ѝ отговорност

2.1.3 всеки инцидент или събитие, изискващо обработване на доказателства, включително:

2.1.3.1 вътрешни заплахи, нарушения на сигурността на данните или разследвания на измами

2.1.3.2 злоупотреба със системи или идентификационни данни

2.1.3.3 инциденти, свързани с оперативни технологии (OT) или индустриални системи за управление

2.1.3.4 нарушения на физическия достъп, засягащи цифрови активи

2.2 Политиката урежда също всяко взаимодействие с външни форензични услуги или правоохранителни органи при правна ескалация или регулаторни производства.

3. Цели

3.1 Да осигури бързо, сигурно и съобразено с политиката придобиване на доказателства при събития по сигурността или разследвания.

3.2 Да запази целостта, автентичността и допустимостта на събраните цифрови доказателства чрез строг контрол на достъпа, регистриране и процедури за проверка.

3.3 Да гарантира, че всички форензични дейности се координират с правните и регулаторните задължения, включително защитата на данните, трудовото право и ограниченията за международен трансфер.

3.4 Да подпомага анализа след инцидент, установяването на първопричината и подобряването на контролите чрез висококачествени форензични резултати.

3.5 Да интегрира форензичната готовност в общата Система за управление на информационната сигурност (СУИС), като подпомага одитите, уведомяването при нарушения и вземането на решения от изпълнителното ръководство.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за настоящата политика и гарантира, че всички форензични дейности са правно обосновани, подлежат на одит и са базирани на риска.

4.1.2 Одобрява ескалацията към външни правни субекти и външни доставчици на форензични услуги.

4.2 Форензични анализатори / служители по реагиране при инциденти

4.2.1 Ръководят придобиването, запазването и техническия анализ на доказателства.

4.2.2 Гарантират, че веригата на съхранение е надлежно документирана и поддържана.

4.2.3 Документират всички действия, констатации и настройки на инструментите, използвани по време на разследванията.

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

9. Преглед и актуализация

9.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно и да се актуализира при необходимост, за да отразява:

9.1.1 промени в закони, регулации или съдебна практика, които засягат форензичните процедури или обработването на данни

9.1.2 актуализации на признати в индустрията форензични стандарти или инструментариум

9.1.3 извлечени поуки от прегледи след инцидент, правни спорове или одитни констатации

9.1.4 технологични промени в платформи, устройства или системи, които са предмет на разследване

9.2 Процесът по преглед е отговорност на директора по информационна сигурност (CISO) и трябва да включва консултации със:

9.2.1 Правни въпроси и съответствие

9.2.2 длъжностното лице по защита на данните (DPO)

9.2.3 екипите по операции по сигурността и форензика

9.2.4 вътрешен одит

9.3 Всички редакции трябва да бъдат:

9.3.1 под управление на версиите и съхранявани в хранилището за политики

9.3.2 комуникирани до засегнатите заинтересовани страни, включително форензичните екипи и екипите за реагиране

9.3.3 придружени от актуализации на съответните оперативни процедури и материали за обучение

9.4 Извънредни прегледи трябва да се задействат след всеки критичен инцидент, свързан с неправилно обработване на доказателства, нарушаване на веригата на съхранение или проблеми с допустимостта по съдебен ред.

10. Свързани политики и връзки

10.1 Настоящата политика е съгласувана със следните организационни политики и се подпомага от тях:

10.1.1 P1 – Политика за информационна сигурност: Установява основния мандат за разследвания, контрол върху доказателствата и съответствие с приложимото законодателство.

10.1.2 P5 – Политика за управление на промените: Гарантира, че системите, които са предмет на разследване, не се променят по време на активни форензични процеси.

10.1.3 P14 – Политика за съхранение и унищожаване на данни: Урегулира сигурното унищожаване и сроковете за съхранение на доказателства и данни, свързани със случаи.

10.1.4 P18 – Политика за криптографски контроли: Определя изискванията за криптиране при съхранение и прехвърляне на чувствителни данни или данни с доказателствена стойност.

10.1.5 P22 – Политика за регистриране и мониторинг: Осигурява наличността на регистрационни файлове за събития и телеметрия за събиране на доказателства и форензична корелация.

10.1.6 P30 – Политика за реагиране при инциденти: Определя триажа на инциденти и пътищата за ескалация, при които се задействат форензични процедури.

10.1.7 P33 – Политика за мониторинг на одита и съответствието: Валидира спазването на форензичните протоколи и изискванията за верига на съхранение чрез регулярни одити.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международните стандарти за форензика и обработване на инциденти, като гарантира целостта на доказателствата, правна обоснованост и съответствие в различни юрисдикции.

11.2 ISO/IEC 27001

11.2.1 Клауза 8.1 – Подпомага оперативния контрол на форензичната готовност и процедурите за работа с доказателства

11.3 ISO/IEC 27002

11.3.1 Приложение A, Контрол 5.25 – Отговорности за управление на инциденти: Изисква определени роли за обработване на инциденти по информационна сигурност и разследвания.

11.3.2 Приложение A, Контрол 5.26 – Докладване на събития по информационна сигурност: Подпомага събирането на артефакти, свързани със събития, като доказателства.

11.3.3 Приложение A, Контрол 5.27 – Реагиране при инциденти по информационна сигурност: Налага структуриран, основан на доказателства подход за ограничаване, отстраняване и разследване.

11.3.4 Приложение A, Контрол 8.27 – Сигурна разработка и форензика (когато е приложимо): Разглежда защитата на системите и инструментите по време на разследвания.

11.4 ISO/IEC 27035:2016 (Части 1 и 3)

11.4.1 Очертава принципите за откриване на инциденти, реагиране и форензична готовност, включително планиране, верига на съхранение и управление на доказателства при инциденти.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 до IR-9, AU-6, PL-2: Определя структурирани изисквания за планиране, откриване, анализ, ограничаване и реагиране при инциденти по сигурността. Подпомага събирането и одитируемостта на доказателствата (AU-6) и гарантира съгласуваност с плановете за сигурност и поверителност на системите (PL-2) по време на форензични разследвания.

11.6 NIST SP 800-86

11.6.1 Предоставя насоки за интегриране на форензичните процеси в по-широкия жизнен цикъл на реагиране при инциденти и за осигуряване на форензична готовност.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Фокусира се върху добрите практики за придобиване, запазване и анализ на цифрови носители и доказателства от мобилни устройства по правно обоснован начин.

11.8 GDPR на ЕС (2016/679)

11.8.1 Член 5 – Принципи, свързани с обработването на лични данни: Прилага се към доказателства, съдържащи лични данни или чувствителни данни, като гарантира минимизиране и ограничаване на целите.

11.8.2 Членове 33–34 – Уведомяване при нарушение на сигурността на данните: Форензичните данни подпомагат съответствието със задълженията за уведомяване при нарушения и процесите по правно разкриване.

11.9 Директива (ЕС) NIS2 (2022/2555)

11.9.1 Член 23 – Задължения за докладване: Форензичната документация и констатациите подпомагат своевременното и точно докладване на инциденти до компетентните органи.

11.10 DORA на ЕС (2022/2554)

11.10.1 Член 17 – Докладване на ИКТ инциденти: Изисква подробни записи за първопричината и доказателствени записи на съществени инциденти, свързани с ИКТ, особено във финансовия сектор.

11.11 COBIT 2019

11.11.1 DSS01.07 – Управление на инциденти по сигурността: Налага документиране на инцидентите и необходимата строгост при разследванията.

11.11.2 DSS05.04 – Управление на разследвания по сигурността: Подчертава запазването на цифрови доказателства и подпомагането на дисциплинарни и правни действия.