					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P31S					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**

Съответствие със стандарти и регулаторни изисквания

Стандарт/регулация	**Клауза/член**	**Коментар**
ISO/IEC 27001:2022	Клаузи 6.1, 6.3, 8	Планиране, основано на риска, действия за подобрение и оперативни контроли за гарантиране целостта на доказателствата
ISO/IEC 27002:2022	Контроли 5.24–5.27	Насоки за сигурно обработване, прегледи след инциденти и подобрения, основани на доказателства
ISO/IEC 27035-3:2016	Клаузи 6.3, 6.4, 7	Осигурява надлежно планиране, законосъобразно събиране и сигурно обработване на цифрови доказателства с документация за веригата на съхранение
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Готовност за форензичен анализ, защита на одитните журнали и ефективна интеграция в реагирането при инциденти
GDPR на ЕС	Членове 33, 34	Документиране и проследимост при нарушения на сигурността на личните данни
NIS2 на ЕС	Член 23	Проследимо докладване на инциденти и сигурно обработване на доказателства
DORA на ЕС	Член 17(1), 17(2)	Осигурява събиране, съхранение и срокове за съхранение на доказателства за инциденти, свързани с ИКТ, форензична надеждност и отговор на регулаторни запитвания
COBIT 2019	DSS05.06, DSS05.07	Надеждно регистриране и структурирано обработване на доказателства за сигурни и подлежащи на одит разследвания

1. Цел

1.1. Настоящата политика определя как организацията обработва цифрови доказателства, свързани с инциденти по информационна сигурност, нарушения на сигурността на данните или вътрешни разследвания. Тя гарантира, че доказателствата се събират, съхраняват и запазват по законосъобразен и годен за одит начин, като подпомагат както вътрешното вземане на решения, така и евентуални външни действия.

1.2. Политиката позволява на малките организации да защитават целостта на журнали, файлове и системни образи, като същевременно демонстрират надлежна грижа съгласно ISO/IEC 27001, GDPR и свързаните стандарти.

1.3. Тя подпомага готовността за форензичен анализ, без да изисква напреднали технически ресурси или собствен ИТ екип на пълен работен ден, чрез определяне на ясни отговорности, процеси и изисквания за съхранение.

2. Обхват

2.1. Настоящата политика се прилага за:

2.1.1. Всички служители, доставчици на ИТ услуги и външни консултанти, участващи в реагиране при инциденти, разследване или анализ на нарушения

2.1.2. Всички фирмени системи, включително лаптопи, мобилни устройства, сървъри, акаунти за електронна поща, SaaS платформи и облачни хранилища (напр. Microsoft 365, Google Workspace)

2.1.3. Всяко събитие, при което са необходими доказателства за вътрешни дисциплинарни действия, правна защита, застрахователни претенции или взаимодействие с регулаторен орган

2.2. Това включва както действителни, така и предполагаеми събития, свързани с:

2.2.1. Изтичане на данни

2.2.2. Вътрешна заплаха или неправомерна употреба

2.2.3. Нарушения на сигурността (напр. зловреден софтуер, неоторизиран достъп)

2.2.4. Жалби от клиенти, изискващи цифрово потвърждение

2.2.5. Запитвания от регулатори или правоохранителни органи

3. Цели

3.1. Да се гарантира, че всички доказателства се събират и обработват по начин, който запазва тяхната целост, автентичност и верига на съхранение.

3.2. Да се предотврати случайна промяна, изтриване или неправилно обработване на журнали, файлове или системни образи, които може да са необходими за разследвания.

3.3. Да се осигури последователен и подлежащ на одит подход към управлението на доказателства, който отговаря на правните и регулаторните очаквания (напр. уведомяване при нарушение по GDPR, проследимост по NIS2).

3.4. Да се определят ясни роли и отговорности, за да се осигури бързо, сигурно и законосъобразно събиране на доказателства по време на инциденти по информационна сигурност.

3.5. Да се подпомогне готовността за форензичен анализ на ниво МСП, като се минимизира сложността и се избягва нарушаване на ежедневната дейност.

4. Роли и отговорности

4.1. Управител

4.1.1. Одобрява всички формални разследвания, които изискват събиране на доказателства.

4.1.2. Преглежда и утвърждава доклади за инциденти, включващи потенциални правни или дисциплинарни действия.

4.1.3. Решава дали следва да бъдат уведомени външен правен консултант или регулатори.

4.1.4. Осигурява редовен преглед и актуализация на политиката.

4.2. Доставчик на ИТ услуги / системен администратор

4.2.1. Събира и запазва цифрови доказателства съгласно сигурни процедури.

4.2.2. Документира времеви маркери, системни параметри и стъпките по обработване.

4.2.3. Осигурява съхранението на всички събрани материали в защитено местоположение.

4.2.4. Съдейства при форензичен анализ, когато е необходимо.

[... 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. Годишен преглед на политиката

9.1.1. Настоящата политика трябва да се преглежда най-малко веднъж на всеки 12 месеца от Управителя, за да се потвърди:

9.1.1.1. Съответствие с контролите от Приложение A на ISO/IEC 27001

9.1.1.2. Продължаваща приложимост към текущите цифрови платформи и ИТ услуги

9.1.1.3. Адекватност на процедурите за регистриране, съхранение на доказателства и готовност за форензичен анализ

9.2. Събития, водещи до преразглеждане на политиката

9.2.1. Политиката трябва също да бъде преглеждана и актуализирана след:

9.2.1.1. Всеки съществен инцидент, изискващ събиране на доказателства

9.2.1.2. Неуспешен одит или регулаторно искане, при което е била поставена под съмнение целостта на доказателствата

9.2.1.3. Внедряване на нови инструменти или процедури за реагиране при инциденти или наблюдение на системите

9.2.1.4. Правни промени (напр. актуализирани указания по GDPR или NIS2)

9.3. Одобрение на промените и разпространение

9.3.1. Всички промени трябва да бъдат прегледани и одобрени от Управителя

9.3.2. Актуализираната версия трябва да бъде споделена със:

9.3.2.1. Доставчици на ИТ услуги и консултанти, участващи в разследвания

9.3.2.2. Всички служители с отговорности по системно администриране

9.3.3. Актуализирано копие трябва да се съхранява в архива на политиките на дружеството и да се предоставя на одитори при поискване

10. Свързани политики и връзки

10.1. Настоящата политика е взаимосвързана със следните политики, съобразени с нуждите на МСП:

10.1.1. P2S – Политика за роли и отговорности в управлението: Установява правомощията във връзка с разследвания на инциденти, решения относно доказателства и правна ескалация.

10.1.2. P4S – Политика за контрол на достъпа: Гарантира, че само упълномощен персонал може да получава достъп до чувствителни системи и журнали по време на разследвания.

10.1.3. P22S – Политика за регистриране и мониторинг: Осигурява първичните данни, използвани като форензични доказателства, и определя изискванията за срокове за съхранение, контрол на достъпа и регистриране.

10.1.4. P30S – Политика за реагиране при инциденти: Инициира необходимостта от събиране на доказателства и определя оперативния поток, водещ до форензично запазване.

10.1.5. P17S – Политика за защита на данните и поверителност: Гарантира, че всички лични данни, събрани като доказателства, се обработват законосъобразно съгласно GDPR и свързаните регулации.

10.2. Тези политики действат съвместно в подкрепа на правната обоснованост, целостта на разследването и пълната готовност за одит по ISO/IEC 27001:2022.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 6.1 – Планирането, основано на риска, включва готовност за реагиране и процедури за работа с доказателства.

11.1.2. Клауза 6.3 – Подпомага действията за подобрение въз основа на доказателства от инциденти.

11.1.3. Клауза 8.1 – Изисква оперативни контроли за целостта на доказателствата.

11.2. ISO/IEC 27002

11.2.1. Контроли 5.24–5.27 – Дават насоки за сигурно обработване, прегледи след инциденти и подобрения, основани на доказателства.

11.3. ISO/IEC 27035-3

11.3.1. Клаузи 6.3, 6.4 и 7.3 – Осигуряват надлежно планиране, законосъобразно събиране и сигурно обработване на цифрови доказателства по време на реагиране при инциденти, включително запазване и документация за веригата на съхранение.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 и AU-12 – Осигуряват готовност за форензичен анализ, защита на одитните журнали и ефективно интегриране на събирането на доказателства в жизнения цикъл на реагиране при инциденти

11.5. NIST SP 800-86

11.5.1. Определя добри практики за придобиване, анализ и защита на цифрови доказателства по време на реагиране при инциденти.

11.6. GDPR на ЕС

11.6.1. Членове 33–34 – Изискват документиране и проследимост на инцидентите и доказателствата при докладване на нарушение на сигурността на личните данни.

11.7. Директива NIS2 на ЕС (2022/2555)

11.7.1. Член 23 – Изисква проследимо докладване на инциденти и сигурно обработване на доказателства за съществени и важни субекти.

11.8. DORA на ЕС

11.8.1. Член 17(1) – Изисква доказателствата, свързани с инциденти, свързани с ИКТ, да се събират и съхраняват по начин, който подпомага форензични разследвания.

11.8.2. Член 17(2) – Изисква финансовите субекти да съхраняват всички относими данни и журнали, свързани със събития по сигурността, в съответствие с изискванията за форензична надеждност и регулаторни запитвания.

11.9. COBIT 2019

11.9.1. DSS05.06 – Наблюдение, откриване и докладване на инциденти: Подчертава значението на надеждното регистриране в подкрепа на разследванията.

11.9.2. DSS05.07 – Разследване и предприемане на действия по инциденти: Изисква структурирано обработване на доказателства, за да се осигурят сигурни и подлежащи на одит разследвания.