					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P14S					Заглавие на документа: **Политика за съхранение и унищожаване на данни**							
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**

Съгласувано с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1.3, 8	Обхваща третиране на риска, оперативни контроли и изисквания за срокове за съхранение
ISO/IEC 27002:2022	Контрол 5	Насоки относно сроковете за съхранение и методите за сигурно унищожаване
NIST SP 800-53 Rev.5	AU-11, MP-6, SI-12	Съхранение на одитни записи, саниране на носители, ограничения и прилагане на сроковете за съхранение на данни
EU NIS2	Член 21(2)(a)	Изисква политика за управление на жизнения цикъл, съобразена с риска
EU DORA	Член 5(1)	Управление на риска в областта на ИКТ: наличност и премахване на данни
COBIT 2019	BAI03.04, DSS01	Контроли за жизнения цикъл на информацията, сигурно унищожаване
EU GDPR	Член 5(1)(e), 17	Данните не се съхраняват по-дълго от необходимото; право на изтриване

1. Цел

1.1 Целта на тази политика е да установи задължителни правила за съхранението и сигурното унищожаване на информация в среда на МСП. Тя гарантира, че записите се съхраняват само за срока, изискуем по закон, по договорно задължение или по служебна необходимост, след което се унищожават по сигурен начин.

1.2 Настоящата политика има за цел да намали информационния риск, да управлява правната експозиция и да ограничи съхранението на излишни или остарели данни. Тя подпомага съответствието с ISO/IEC 27001 и рамки за защита на личните данни като GDPR чрез минимизиране на неразрешеното съхранение на лична или чувствителна информация.

1.3 Добре структурираната рамка за съхранение и унищожаване намалява оперативните разходи, подобрява производителността на системите и повишава готовността за одит. За МСП с ограничен ИТ капацитет тя осигурява практически подход за отговорно управление на цифрови и физически информационни активи.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 всички записи, файлове, журнали, комуникации и масиви от данни, създадени, събрани, обработвани или съхранявани от организацията

2.1.2 всички служители, външни изпълнители и доставчици, които обработват организационни данни

2.1.3 всички формати на данни (напр. хартиени, електронни, изображения, аудио или журнални записи) и всички носители за съхранение (напр. локални дискове, облачни услуги, пощенски сървъри, резервни копия)

2.2 Обхватът включва:

2.2.1 бизнес документи (напр. фактури, договори, проектни отчети)

2.2.2 оперативни записи (напр. журнали, история на достъпа, моментни снимки на резервни копия)

2.2.3 лични данни (напр. досиета по човешки ресурси, комуникации с клиенти, записи по поддръжка)

2.2.4 данни, хоствани вътрешно, външно или в хибридни системи

2.2.5 архивирани данни и резервни копия, независимо дали са активни или неактивни

2.3 Всички етапи от жизнения цикъл на данните са в обхвата — от създаването до разрешеното унищожаване.

3. Цели

3.1 Да се определят последователни правила за съхранение въз основа на правни, оперативни и регулаторни критерии.

3.2 Да се предотврати преждевременното изтриване на критични записи и да се елиминира ненужното натрупване на данни.

3.3 Да се осигури сигурно и необратимо унищожаване на данни, когато съхранението им вече не е необходимо.

3.4 Да се възложи отговорност за прилагане на решенията за съхранение и изтриване в условията на ограничения в персонала, характерни за МСП.

3.5 Да се осигури документация, годна за одит, за доказване на надлежна грижа съгласно ISO/IEC 27001, GDPR, NIS2 и други рамки.

3.6 Да се насърчава сигурното управление на данните през целия им жизнен цикъл, без да се създава ненужно техническо натоварване за персонал без специализирана експертиза.

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява тази политика и носи цялостна отговорност за нея.

4.1.2 Осигурява внедряването на процедури за съхранение и унищожаване по начин, съобразен с правния и бизнес риска.

4.1.3 Одобрява изключения и правно задържане, когато е необходимо.

4.1.4 Инициира прегледи на политиката и одобрява актуализации въз основа на промени в бизнеса или регулаторната среда.

4.2 Определен собственик на данни

4.2.1 Определя се за всяка категория данни (напр. финансови, по човешки ресурси, клиентски записи).

4.2.2 Класифицира записите и определя подходящия срок за съхранение въз основа на политиката и правните указания.

4.2.3 Одобрява изтриването, когато изискванията за съхранение са изпълнени.

4.2.4 Подпомага вътрешния одит, като предоставя контекст относно основанията за съхранение и събитията по унищожаване.

[... 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 най-малко веднъж годишно или при:

9.1.1 промени в приложимото законодателство (напр. защита на данните, финансово отчитане)

9.1.2 въвеждане на нови системи или процеси, които засягат жизнения цикъл на данните

9.1.3 одитни констатации или инциденти, които разкриват пропуски в практиките за съхранение

9.2 Прегледите трябва да гарантират, че Регистърът на сроковете за съхранение остава пълен и отразява всички основни категории записи.

9.3 Актуализациите на политиката трябва да бъдат одобрени от Управителя и доведени до знанието на засегнатия персонал. Най-актуалната версия трябва да бъде достъпна и да се поддържа под контрол на версиите.

10. Свързани политики и връзки

10.1 P2S – Политика за роли и отговорности в управлението: Определя собствеността върху политиката и правомощията за изключения.

10.2 P13S – Политика за класификация и етикетиране на данни: Определя как правилата за съхранение се съгласуват с класификацията на данните.

10.3 P12S – Политика за управление на активите: Регулира носителите за съхранение, съдържащи данни, подлежащи на съхранение/унищожаване.

10.4 P17S – Политика за защита на данните и поверителност: Осигурява минимизиране на данните и подпомага законосъобразното обработване съгласно GDPR.

10.5 P30S – Политика за реагиране при инциденти: Активира се, когато пропуски при унищожаване или съхранение водят до потенциална експозиция на данни.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1.3: Изисква третиране на рискове, свързани с информацията, включително рискове, свързани със съхранението.

11.1.2 Клауза 8.1: Определя оперативни контроли за жизнения цикъл.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.33: Насоки за определяне на срокове за съхранение и методи за сигурно унищожаване.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Изисква съхранение на одитни записи.

11.3.2 MP-6: Определя процедури за саниране на носители.

11.3.3 SI-12: Разглежда ограниченията и прилагането на сроковете за съхранение на данни.

11.4 EU GDPR

11.4.1 Член 5(1)(e): Данните трябва да се съхраняват не по-дълго от необходимото.

11.4.2 Член 17: Правото на изтриване се прилага, когато данните вече не се съхраняват законосъобразно.

11.5 EU NIS2

11.5.1 Член 21(2)(a): Изисква организационни политики, съобразени с риска, включително управление на жизнения цикъл.

11.6 EU DORA

11.6.1 Член 5(1): Управлението на риска в областта на ИКТ включва наличност и премахване на данни.

11.7 COBIT 2019

11.7.1 BAI03.04: Изискват се контроли за жизнения цикъл на информацията.

11.7.2 DSS01.06: Процедури за сигурно унищожаване като част от защитата на информационните активи.