					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P14					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**

Съответствие със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1.3, 8.1	
ISO/IEC 27002:2022	Контроли 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
GDPR на ЕС	Членове 5(1)(e), 17, 32	
NIS2 на ЕС	Член 21(2)(a-e)	
DORA на ЕС	Членове 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Цел

1.1 Целта на настоящата политика е да определи организационните изисквания за съхранение на данни и сигурното им унищожаване през всички етапи от жизнения цикъл на информацията. Тя осигурява съответствие с приложимите правни, регулаторни и договорни задължения и предотвратява ненужно или рисково натрупване на данни.

1.2 Настоящата политика подпомага прилагането на ISO/IEC 27001:2022 чрез установяване на контрол върху сроковете за съхранение на данни и практиките за необратимо унищожаване. Тя осигурява проследима документация на записите, налага срокове за съхранение, съобразени с чувствителността съгласно класификацията, и гарантира готовност за одит, регулаторна проверка и представяне на доказателства в рамките на съдебни производства.

1.3 Политиката има за цел също да защитава поверителността, целостта и наличността на данните, като същевременно свежда до минимум бизнес риска, оперативните неефективности и експозицията към нарушения на сигурността и поверителността, произтичащи от неправилно съхранение или унищожаване на данни.

2. Обхват

2.1 Настоящата политика се прилага за всички физически и цифрови информационни активи, които са притежавани, обработвани или съхранявани от организацията, включително активи под контрола на трети страни, дъщерни дружества или аутсорсинг партньори.

2.2 Обхватът включва, без да се ограничава до:

2.2.1 Документи, файлове и записи (в цифров и хартиен формат)

2.2.2 Бази данни и архиви

2.2.3 Електронна поща и журнали от незабавни съобщения

2.2.4 Архивни копия, системни журнали и одитни следи

2.2.5 Изходен код, данни от приложения и активи, хоствани в облачна среда

2.2.6 Сменяеми носители и изведен от употреба хардуер, съдържащ данни

2.3 Политиката урежда както оперативните записи, така и регулираните набори от данни (напр. финансово, правно, ЧР, клиентско и относимо към одит съдържание), независимо от мястото за съхранение или използваната система.

2.4 Тя се прилага за всички организационни звена, както и за служители, външни изпълнители и доставчици, ангажирани със създаването, съхранението, управлението или унищожаването на данни.

3. Цели

3.1 Да се гарантира, че данните се съхраняват само толкова дълго, колкото е необходимо по закон, договор или оперативна необходимост, и се унищожават сигурно, когато вече не са необходими.

3.2 Да се предотврати преждевременно, неоторизирано или случайно изтриване на записи, необходими за текущи операции, съответствие, съдебно производство или одитни цели.

3.3 Да се установят и прилагат последователни графици за съхранение въз основа на класификацията на данните, вида на актива, приложимото законодателство и рисковата експозиция.

3.4 Да се защити неприкосновеността на личния живот и поверителността на данните по време на срока за съхранение и при унищожаването, включително чрез упражняване на правата на субектите на данни (напр. изтриване съгласно член 17 от GDPR).

3.5 Да се гарантира, че всички методи за унищожаване на данни са необратими, надлежно документирани и съответстват на признати стандарти, като NIST SP 800-88.

3.6 Да се сведат до минимум оперативните неефективности, допълнителните разходи и правната експозиция, причинени от прекомерно съхранение или непроследени наследени данни.

3.7 Да се подпомогнат целите за непрекъсваемост на дейността и възстановяване при бедствия чрез интегрирано управление на сроковете за съхранение на архивните копия и защитими практики за архивиране на данни.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява настоящата политика и осигурява подходящо финансиране, ресурси и интегриране в програмите за управление на корпоративния риск и съответствието.

4.1.2 Носи цялостна отчетност за правното и регулаторното съответствие, свързано със съхранението на данни и сигурното унищожаване.

4.2 Директор по информационна сигурност (CISO)

4.2.1 Отговаря за настоящата политика и носи отговорност за определянето и прегледа на управлението на съхранението и унищожаването в съответствие със Системата за управление на информационната сигурност (СУИС).

4.2.2 Осигурява внедряването на изискванията за съхранение и унищожаване, определени от класификацията, в бизнес звената и техническите системи.

4.2.3 Наблюдава спазването на политиката и инициира коригиращи действия, 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 Настоящата политика трябва да се преглежда ежегодно или при настъпване на някое от следните условия:

9.1.1 Промени в приложимите закони или регулации, които засягат съхранението на данни (напр. актуализации на GDPR, данъчни кодекси, DORA)

9.1.2 Промени в рамката за класификация или в бизнес процесите, които оказват влияние върху етапите от жизнения цикъл на данните

9.1.3 Въвеждане на нови ИТ системи, платформи за архивиране или технологии за унищожаване на носители

9.1.4 Констатации от вътрешен одит или регулаторни препоръки, които подчертават пропуски в практиките за съхранение или унищожаване

9.2 Прегледът трябва да се ръководи от CISO и Длъжностното лице по защита на данните (DPO), с участието на Правни въпроси и съответствие, ИТ и бизнес звената.

9.3 Главният график за съхранение на данни (MDRS) и Регистърът за унищожаване трябва да се преглеждат паралелно, за да се гарантира, че:

9.3.1 Графиците остават точни и отразяват оперативните, правните и регулаторните нужди

9.3.2 Документацията за унищожаване е пълна и подлежи на одит

9.3.3 Записите за правно задържане са валидирани и освобождавани, когато е уместно

9.4 Всички актуализации на политиката трябва:

9.4.1 Да бъдат формално управлявани чрез контрол на версиите и съхранявани в хранилището за документи на СУИС

9.4.2 Да включват история на промените и обосновка за промените

9.4.3 Да бъдат одобрени от Изпълнителното ръководство

9.4.4 Да бъдат комуникирани на съответния персонал с актуализирани обучителни или указателни материали

9.5 Когато настъпят съществени промени в политиката, засегнатите служители трябва да преминат целево обучение в срок до 30 дни от публикуването, за да се гарантира продължаващо съответствие.

9.6 Свързани политики и връзки

10. Свързани политики и връзки

10.1.1 P4 - Политика за контрол на достъпа: Гарантира, че само упълномощени лица имат достъп до данните по време на срока им за съхранение и че данните с изтекъл срок са ограничени до унищожаването им.

10.1.2 P12 - Политика за управление на активите: Определя кои активи съдържат данни, изискващи планирано унищожаване, и проследява жизнения им цикъл от придобиването до унищожаването.

10.1.3 P13 - Политика за класификация и етикетиране на данните: Насочва решенията по класификация, които пряко влияят върху продължителността на съхранение на данните и изисквания метод за унищожаване.

10.1.4 P15 - Политика за архивни копия и възстановяване: Определя сроковете за съхранение и процедурите за унищожаване на носители за архивни копия и репликирани информационни активи.

10.1.5 P18 - Политика за криптографски контроли: Поддържа криптографско изтриване за целите на унищожаването и налага криптиране при съхранение на данните до тяхното унищожаване.

10.1.6 P30 - Политика за реагиране при инциденти: Задейства се в случаи, когато неправилното унищожаване води до потенциална загуба на данни, инцидент по информационна сигурност или регулаторно нарушение.

10.2 Всяка свързана политика има роля за прилагането на съгласуван модел за управление на данните по отношение на класификацията, контрола върху жизнения цикъл, достъпа и готовността за одит.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати стандарти и регулаторни рамки, които определят сигурни, съответстващи и ефективни практики за управление на жизнения цикъл на данните.

11.2 ISO/IEC 27001:

11.2.1 Клауза 6.1.3 - План за третиране на риска: Подпомага смекчаването на рисковете, свързани с прекомерно съхранение, нарушения на сигурността на данните или неуспехи при унищожаване.

11.2.2 Клауза 8.1 - Оперативно планиране и контрол: Установява контроли по жизнения цикъл, които уреждат съхранението, архивирането и унищожаването.

11.3 ISO/IEC 27002:2022 - Контроли 5.10, 5.12, 5.30, 5: Предоставят практически насоки за допустима употреба на данни, обосновка за съхранение, контролирано изтриване и защитимо водене на записи в съответствие с толеранса към риска на организацията.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Съхранение на одитни записи: Осигурява достатъчно съхранение на одитни журнали и доказателства за съответствие.

11.4.2 MP-6 - Саниране на носители: Изисква сигурни и документирани методи за унищожаване на физически и електронни носители.

11.4.3 SI-12 - Обработване на информация: Налага подходящо третиране на данните в съответствие с контролите за съхранение и унищожаване.

11.4.4 PL-2 - План за сигурност и защита на поверителността на системата: Изисква специфична за системата документация за обработването през жизнения цикъл на данните и мерките за сигурно унищожаване.

11.5 GDPR на ЕС (2016/679):

11.5.1 Член 5(1)(e) - Минимизиране на данните и ограничение на съхранението: Изисква данните да не се съхраняват по-дълго от необходимото.

11.5.2 Член 17 - Право на изтриване („право да бъдеш забравен“): Изисква своевременно и окончателно изтриване на лични данни при валидно искане.

11.5.3 Член 32 - Сигурност на обработването: Засилва защитата на данните по време на съхранението и изисква сигурно унищожаване на записи с изтекъл срок.

11.6 Директива NIS2 на ЕС (2022/2555):

11.6.1 Член 21(2)(a-e): Изисква организациите да приемат политики и технически мерки за сигурно обработване на данни, включително ограничения за съхранение и методи за унищожаване.

11.7 DORA на ЕС (2022/2554):

11.7.1 Член 5 - Управление и контрол: Налага структурирано управление на ИКТ риска, включително сигурно управление на информацията през жизнения ѝ цикъл.

11.7.2 Член 9 - Рамка за управление на ИКТ риска: Изисква политики за съхранение на данни, унищожаване и правно/регулаторно съответствие на цифровите операции.

11.8 COBIT 2019:

11.8.1 DSS01 - Управлявани операции: Подпомага проследяването на съхранението и последователността в системите за данни.

11.8.2 DSS05 - Управлявани услуги по сигурността: Осигурява защита на съхраняваните и архивираните данни до тяхното сигурно унищожаване.

11.8.3 MEA03 - Мониторинг, оценяване и преценка на съответствието: Позволява одитиране на прилагането на сроковете за съхранение, процедурите за изтриване и изпълнението на регулаторните изисквания.