					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P13S					Заглавие на документа: **Политика за класификация и етикетиране 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**

Правна бележка (авторски права и ограничения за ползване)

(C) 2025 Clarysec LLC. All rights reserved.

Настоящият документ е интелектуална собственост на Clarysec LLC. Никоя част от него не може да бъде копирана, използвана повторно, разпространявана или изменяна за търговски или внедрителски цели без изрично писмено разрешение.

Неупълномощеното използване е строго забранено и може да доведе до правни действия.

За лицензиране се свържете с: info@clarysec.com

Съгласуваност с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 5.3, 8	
ISO/IEC 27002:2022	Контроли 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
Директива NIS2 на ЕС	Член 21(2)(a)	
Регламент DORA на ЕС	Член 5(8)	
COBIT 2019	BAI03.05, DSS05	
Регламент (ЕС) 2016/679 (GDPR)	Членове 5, 32	

1. Цел

1.1 Настоящата политика определя как цялата информация, обработвана от организацията, трябва да бъде класифицирана и етикетирана, за да се гарантира, че нейната поверителност, цялостност и наличност се поддържат през целия ѝ жизнен цикъл.

1.2 Политиката осигурява последователно обработване на данните чрез определяне на подходящи нива на защита на информацията въз основа на нейната чувствителност, въздействието върху дейността или приложимите правни задължения.

1.3 Класификацията и етикетирането подпомагат намаляването на риска от случайно разкриване, неоторизиран достъп или неправомерно боравене с чувствителни данни, особено в МСП, които може да разчитат на по-опростени системи и по-слабо формализирани контроли.

1.4 Настоящата политика е съществена за сертифициране по ISO/IEC 27001 и за регулаторното съответствие, по-специално с изискванията за защита на данните съгласно GDPR и с рамките за киберсигурност като NIS2 и DORA.

2. Обхват

2.1 Настоящата политика се прилага за всички организационни данни, независимо от техния формат или местонахождение, включително:

2.1.1 Електронни документи, електронни таблици, електронна поща, формуляри, изображения и сканирани файлове

2.1.2 Физически документи, включително разпечатки, отчети, фактури и бележки

2.1.3 Данни, съхранявани или обработвани в облачни услуги, на локални сървъри, върху сменяеми носители или на лично притежавани устройства, използвани за служебни цели

2.1.4 Временни или преходни данни, генерирани в хода на бизнес операциите (напр. журнали, кеш файлове, електронна поща)

2.2 Всички служители, външни изпълнители, временни работници и външни доставчици с достъп до организационни данни са длъжни да спазват настоящата политика.

2.3 Политиката се прилага през целия жизнен цикъл на данните — от създаването и съхранението, през достъпа и прехвърлянето, до архивирането или изтриването.

3. Цели

3.1 Да се определи опростена и приложима схема за класификация, която може лесно да бъде разбрана и прилагана в цялата организация.

3.2 Да се изисква всеки информационен актив или масив от данни да бъде класифициран според неговата чувствителност и съответно етикетиран, за да се осигури правилното му обработване, съхранение и достъп.

3.3 Да се гарантира, че практиките за етикетиране на данни са интегрирани в бизнес процеси като въвеждане в длъжност, стартиране на проекти и конфигуриране на системи.

3.4 Да се намали рискът от инциденти, свързани със сигурността на данните, чрез прилагане на контроли за обработване (напр. криптиране, ограничаване на достъпа) според нивото на класификация.

3.5 Да се осигури съответствие с изискванията за защита на личните данни и информационна сигурност чрез доказване, че чувствителните данни (напр. лични, финансови или фирмени) са надлежно етикетирани и управлявани.

3.6 Да се установи отчетност за решенията по класификация и да се осигурят периодични прегледи и актуализации въз основа на променящите се бизнес и правни потребности.

4. Роли и отговорности

4.1 Управител

4.1.1 Отговаря за настоящата политика и одобрява схемата за класификация.

4.1.2 Осигурява надзор, така че отговорностите по класификация да бъдат ясно възложени и изпълнявани.

4.1.3 Преглежда и одобрява всички изключения от изискванията за класификация или етикетиране.

4.1.4 Осигурява практиките по обработване на данни да съответстват на приложимите нормативни изисквания, включително по GDPR и DORA.

4.2 Собственик на информация / Мениджър данни

4.2.1 Определя първоначалната класификация за всеки нов масив от данни или информационен актив при неговото създаване или придобиване.

4.2.2 Осигурява прилагането на видими етикети, когато е приложимо (напр. горни колонтитули, долни колонтитули, водни знаци, имена на папки).

4.2.3 Преглежда периодично класификациите, за да потвърди тяхната актуалност, точност и необходимост от промени (напр. след декласификация или публикуване).

4.2.4 Работи съвместно с ИТ ръководителя за прилагане на технически мерки за защита съобразно класификацията (напр. права за достъп, криптиране).

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

9. Изисквания за преглед и актуализиране

9.1 Настоящата политика трябва да се преглежда ежегодно от Управителя и Мениджъра на данни, за да се гарантира, че отразява:

9.1.1 Промени в бизнес операциите или видовете данни

9.1.2 Нови регулаторни изисквания (напр. относно защитата на личните данни или финансовия надзор)

9.1.3 Технологични промени, засягащи възможностите за етикетиране или класификация

9.2 Прегледът трябва да включва актуализации на категориите за класификация, инструментите или практиките за етикетиране и съдържанието за осведоменост и обучение.

9.3 Промените в политиката трябва да бъдат одобрени от Управителя и комуникирани до целия персонал. За целите на одита трябва да се съхранява история на промените по версии.

10. Свързани политики и зависимости

10.1 P2S – Политика за роли и отговорности в управлението: Определя отчетността за собствеността върху политиките и тяхното прилагане.

10.2 P4S – Политика за контрол на достъпа: Съгласува системния достъп с нивата на класификация на данните.

10.3 P12S – Политика за управление на активите: Проследява физическите и цифровите активи, които съхраняват класифицирани данни.

10.4 P17S – Политика за защита на данните и поверителност: Регламентира защитата на личните данни, голяма част от които са класифицирани като „Поверителна“.

10.5 P30S – Политика за реагиране при инциденти: Определя пътищата за ескалация и процедурите за реагиране при нарушения на класификацията или разкриване на данни.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 5.3: Изисква ясно определени отговорности за обработване и защита на данните.

11.1.2 Клауза 8.1: Изисква оперативно планиране и контроли, включително свързаните с класификацията на данните.

11.2 ISO/IEC 27002

11.2.1 Контрол 5.12: Предоставя насоки за класификация на информацията въз основа на риска и регулаторните изисквания.

11.2.2 Контрол 5.13: Описва практически механизми за етикетиране и свързаните с тях правила за обработване.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: Изисква маркиране на информацията, за да се гарантира, че мерките за защита са съгласувани с класификацията.

11.3.2 MP-3 / MP-5: Предоставят насоки за етикетиране и контрол на носители и изходни материали.

11.4 GDPR

11.4.1 Членове 5 и 32: Изискват минимизиране на данните и гарантиране на цялостност чрез подходящи мерки за класификация и обработване.

11.5 NIS2

11.5.1 Член 21(2)(a): Изисква технически и организационни мерки за защита на данните, базирани на риска.

11.6 DORA

11.6.1 Член 5(8): Изисква организациите да класифицират информационните активи като част от програмата си за управление на ИКТ риска.

11.7 COBIT 2019

11.7.1 BAI03.05: Изисква класификация на информацията и защита, съобразена с риска.

11.7.2 DSS05.02: Разглежда прилагането на контроли, базирани на класификацията, и мониторинга.