					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P13					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**

1. Цел

1.1 Настоящата политика определя формалната рамка за класификация и етикетиране на информационните активи на организацията въз основа на тяхната чувствителност, рискова експозиция и регулаторни задължения.

1.2 Тя гарантира, че цялата информация — независимо дали се съхранява, предава или обработва — е ясно класифицирана и етикетирана по начин, който указва необходимото ниво на защита и правилата за боравене с нея.

1.3 Политиката налага структурирана класификация, съгласувана с практиките на организацията за управление на риска, в подкрепа на целите за поверителност, цялостност и наличност както за цифрови, така и за физически типове данни.

1.4 Този контрол е съществен за осигуряване на ролево базиран достъп, готовност за одит, подходящо споделяне на данни и ефективно прилагане на технически защитни мерки като криптиране, архивиране и мониторинг.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 всички информационни активи на организацията, включително документи, бази данни, записи и комуникации;

2.1.2 всички формати на данни, включително цифрови, печатни, писмени или устни;

2.1.3 всички среди: локални, отдалечени, мобилни и облачни;

2.1.4 всички служители, външни изпълнители, доставчици на услуги и обработващи лични данни трети страни, които създават, обработват или съхраняват информация на организацията.

2.2 Обхватът включва вътрешно разработено съдържание, данни от външни източници, лични данни, попадащи в обхвата на задължения по законодателството за защита на личните данни (напр. GDPR), както и информация, обменяна с клиенти, партньори и регулатори.

2.3 Тя се прилага за всички системи, използвани за съхраняване или предаване на данни, включително корпоративни приложения, файлови сървъри, системи за електронна поща, облачни платформи и хранилища за резервни копия.

3. Цели

3.1 Да установи стандартизирана, общоорганизационна схема за класификация, основана на въздействието от разкриване или компрометиране на данните.

3.2 Да гарантира, че цялата информация е видимо и трайно етикетирана, така че да отразява нивото си на класификация и изискванията за боравене.

3.3 Да наложи контроли за обработване на данни и контрол на достъпа, съобразени с класификацията, включително криптиране, регистриране на събития, защита при предаване и планиране на сроковете за съхранение.

3.4 Да подпомогне съответствието с международни стандарти (ISO/IEC 27001, 27002), правни рамки (GDPR, NIS2, DORA) и вътрешни политики за управление на риска.

3.5 Да гарантира, че всички потребители разбират своите отговорности за защита на данните, прилагане на етикети и правилно боравене с класифицирана информация.

3.6 Да поддържа проследимост между статуса на класификация, свързаните контроли и Инвентара на активите на организацията за целите на одита и съответствието.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за политиката за класификация и етикетиране на информацията и гарантира съответствието ѝ с регулаторните, договорните и оперативните изисквания.

4.1.2 Одобрява нивата на класификация, стандартите за етикетиране и промените в политиката.

4.1.3 Осъществява надзор върху спазването на политиката чрез одити, показатели и преглед на изключенията.

4.1.4 Координира междуфункционалното управление с екипите по правни въпроси, защита на личните данни и управление на риска.

4.2 Собственици на информация

4.2.1 Отговарят за класифицирането на информационните активи под техен контрол, като използват организационната схема за класификация.

4.2.2 Прилагат етикети за класификация при създаване, актуализиране или приемане на информация.

4.2.3 Периодично преглеждат класификацията на активите, особено при промени в чувствителността, регулаторния обхват или бизнес стойността.

4.2.4 Гарантират, че чувствителните данни се обработват и етикетират по подходящ начин през целия им жизнен цикъл.

[... 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 Настоящата политика трябва да се преглежда най-малко веднъж годишно, за да се гарантира съгласуваност с:

9.1.1 развиващите се регулаторни изисквания (напр. GDPR, NIS2, DORA);

9.1.2 актуализациите на указанията за класификация по ISO/IEC 27001 или 27002;

9.1.3 организационни промени, засягащи чувствителността на данните или собствеността върху тях;

9.1.4 технологични промени, включително нови платформи за управление на документи или данни.

9.2 Директорът по информационна сигурност (CISO) трябва да инициира прегледа в сътрудничество с Комитета по информационна сигурност, правния консултант и засегнатите бизнес звена.

9.3 Прегледите трябва да включват:

9.3.1 ефективността на прилагането на класификацията и спазването от страна на потребителите;

9.3.2 анализ на инциденти или изключения, свързани с неправилна класификация;

9.3.3 обратна връзка от потребителите относно инструментите за етикетиране или указателните материали;

9.3.4 сравнителен анализ спрямо стандартите за класификация в индустрията.

9.4 Актуализациите на политиката трябва да се управляват чрез контрол на версиите, да се документират в хранилището на СУИС и да се съобщават на целия приложим персонал с акцент върху новите отговорности или промените в инструментите.

9.5 Новоназначените служители трябва да бъдат запознати с текущата версия на политиката по време на въвеждане в длъжност. Всички служители трябва да преминават опреснително обучение след съществени промени в политиката.

10. Свързани политики и връзки

10.1 Настоящата политика е пряко подкрепена от и налага контроли, описани в следните свързани политики:

10.1.1 P4 - Политика за контрол на достъпа: Достъпът до информация се управлява според нивата на класификация; по-чувствителните данни изискват по-строг контрол на достъпа и механизми за оторизация.

10.1.2 P11 - Политика за управление на потребителски акаунти и привилегии: Подсилва разпределянето на привилегии въз основа на необходимостта да се знае, която се определя от нивата на класификация.

10.1.3 P12 - Политика за управление на активите: Гарантира, че всеки актив в инвентара съдържа своята класификация и етикет, като подпомага проследимостта и отчетността.

10.1.4 P14 - Политика за съхранение и унищожаване на данни: Правилата за унищожаване и срокът за съхранение се определят от нивото на класификация на данните и регулаторните изисквания за съхранение.

10.1.5 P18 - Политика за криптографски контроли: Прилага подходящи стандарти за криптиране въз основа на класификацията на информационния актив.

10.1.6 P22 - Политика за регистриране и мониторинг: Осигурява наблюдение на достъпа до и движението на класифицирана информация, като гарантира възможност за одит и откриване на неправилно етикетиране или злоупотреба.

10.2 Всяка връзка гарантира последователна защита на информацията през целия ѝ жизнен цикъл — от създаване и класификация до сигурно боравене, съхранение, предаване и окончателно унищожаване.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати стандарти и регулаторни рамки, уреждащи класификацията и етикетирането на чувствителна информация.

11.2 ISO/IEC 27001

11.2.1 Клауза 4.2 - Разбиране на потребностите и очакванията на заинтересованите страни. Изискванията за класификация често произтичат от правни, регулаторни или договорни задължения, наложени от заинтересовани страни (напр. GDPR, клиентски споразумения за неразкриване на информация (NDA)), които трябва да бъдат отразени в политиката.

11.2.2 Клауза 6.1.3 - Третиране на риска за информационната сигурност. Класификацията пряко влияе върху избора на контроли за третиране на риска, включително контрол на достъпа, криптиране и срок на съхранение, въз основа на чувствителността на данните.

11.2.3 Клауза 7.2 - Компетентност. Политиката изисква персоналът, отговорен за класификацията и етикетирането, да бъде обучен, което попада в обхвата на изискванията за компетентност.

11.2.4 Клауза 7.3 - Осведоменост. Политиката изисква всички потребители да са запознати с нивата на класификация и своите отговорности при боравене с информация, в съответствие със задълженията за осведоменост.

11.2.5 Клауза 7.5 - Документирана информация. Самата политика за класификация е контролиран документ, а процедурите, записите от обучението и етикетите за класификация са част от документираната информация.

11.2.6 Клауза 8.1 - Оперативно планиране и контрол. Класификацията и етикетирането са оперативни процеси, вградени в управлението на жизнения цикъл на данните, а тази клауза гарантира, че такива дейности се планират, внедряват и контролират.

11.2.7 Клауза 9.1 - Мониторинг, измерване, анализ и оценяване. Политиката включва разпоредби за наблюдение на съответствието по класификацията, тенденциите при инцидентите и ефективността на схемата за етикетиране.

11.2.8 Клауза 10.1 - Несъответствие и коригиращо действие. Политиката определя реакциите при неправилна класификация, включително коригиращи действия като повторно обучение, актуализации и обработване на изключения.

11.3 ISO/IEC 27002:2022

11.3.1 Контрол 5.12 - Класификация на информацията. Този контрол гарантира, че информацията се класифицира въз основа на нейната чувствителност, стойност и критичност — именно това формализира настоящата политика.

11.3.2 Контрол 5.13 - Етикетиране на информацията. Този контрол изисква подходящо етикетиране на информацията в съответствие с нейното ниво на класификация, което е изцяло обхванато от политиката.

11.3.3 Контрол 5.10 - Допустимо използване на информационни и други свързани активи. Политиката налага начина, по който потребителите трябва да боравят с класифицирани данни, като пряко подкрепя допустимата употреба и предотвратява злоупотреба.

11.3.4 Контрол 5.11 - Връщане на активи. Класификацията спомага чувствителните данни да бъдат идентифицирани и сигурно върнати или санирани при напускане на служител или доставчик.

11.3.5 Контрол 5.9 - Инвентар на информацията и други свързани активи. Класификацията често е свързана с Инвентара на активите, който трябва да отразява нивото на класификация на всеки елемент с цел правилно разпределяне на контролите.

11.3.6 Контрол 5.14 - Прехвърляне на информация. Нивата на класификация влияят върху контролите при вътрешно и външно прехвърляне на данни (напр. криптиране, одобрение, ограничения на достъпа).

11.3.7 Контрол 8.12 - Предотвратяване на изтичане на данни. Налагането на класификация и етикетиране подпомага предотвратяването на неразрешено разкриване и загуба на данни.

11.3.8 Контрол 8.11 - Маскиране на данни. Някои нива на класификация (напр. Поверителен, Ограничен) могат да изискват маскиране, когато данните се използват в тестови, развойни среди или за аналитични цели.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - Политика и процедури за защита на системите и комуникациите: Подкрепя политиките за класификация като част от цялостната защита на данните.

11.4.2 AC-16 - Атрибути за сигурност: Реализира налагане на достъп въз основа на метаданни за класификация и потребителски разрешения.

11.4.3 MP-3 / MP-5 - Маркиране на носители и защита при транспортиране: Налага етикетиране и защита на данните при съхранение и пренос според класификацията.

11.5 EU GDPR (2016/679)

11.5.1 Член 5 - Принципи за защита на данните: Изисква личните данни да се обработват сигурно и пропорционално на тяхната чувствителност.

11.5.2 Член 32 - Сигурност на обработването: Подсилва класификацията като механизъм за защита на данните, базиран на риска, и за прилагане на подходящи технически мерки.

11.6 Директива ЕС NIS2 (2022/2555)

11.6.1 Член 21(2)(a): Изисква политики за управление на риска за информационната сигурност, включително контроли за класификация на активи и данни.

11.6.2 Член 21(3): Насърчава приемането на мерки за налагане на подходящо боравене с данни — подпомогнато чрез етикетиране, базирано на класификация.

11.7 EU DORA (2022/2554)

11.7.1 Член 5 - Управление и контрол: Изисква рамки за управление, които класифицират активите с данни за целите на контрола на риска в областта на ИКТ.

11.7.2 Член 9 - Управление на риска в областта на ИКТ: Налага технически и организационни мерки за критични ИКТ активи, включително класификация и етикетиране.

11.8 COBIT 2019

11.8.1 DSS05.02 - Управление на услугите по сигурност: Налага класификации по информационна сигурност, за да се гарантира защитата на корпоративните данни.

11.8.2 MEA03 - Мониторинг, оценяване и преценка на съответствието: Подпомага редовния одит и преглед на практиките за класификация, за да се гарантира спазването на политиката и зрелостта.