					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P33S					Заглавие на документа: **Политика за одит и мониторинг на съответствието**							
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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 9.2, 10	Вътрешен одит, непрекъснато подобрение и отстраняване на несъответствия
ISO/IEC 27002:2022	Контроли 5.35, 5.37	Планирани вътрешни прегледи, независими прегледи на външно възложени процеси
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Оценки на сигурността, непрекъснато наблюдение, преглед, анализ и докладване на одита
GDPR на ЕС	Членове 24 и 32	Одитиране на техническите и организационните мерки и доказателства за ефективността на контролите
Директива NIS2 на ЕС	Член 21(2)(f)	Проактивен преглед и съответствие, основано на доказателства
Регламент DORA на ЕС	Член 10	Управление на риска в областта на ИКТ, мониторинг и докладване
COBIT 2019	MEA01, MEA03	Мониторинг и оценка на съответствието, готовност за прегледи от трети страни

1. Цел

1.1 Настоящата политика определя подхода на организацията за извършване на вътрешен одит, проверки на контролите за сигурност и мониторинг на регулаторното съответствие. Тя гарантира, че всички контроли, политики, системи и външни доставчици на услуги подлежат на редовен и структуриран преглед.

1.2 Целта е да се установяват откази на контроли, да се предотвратява несъответствие и да се демонстрира дължима грижа съгласно ISO/IEC 27001, GDPR и свързаните рамки.

1.3 Политиката дава възможност на МСП да поддържат оперативен контрол и готовност за сертификация дори без обособен екип по съответствие, чрез използване на прости, повтаряеми контролни списъци и констатации, приоритизирани според риска.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички вътрешни отдели и външни доставчици на услуги с отговорности, свързани с ИТ системи, лични данни и критични за бизнеса услуги

2.1.2 Всички контроли и системи в обхвата на СУИС

2.1.3 Всички вътрешни одити, прегледи на контролите за сигурност и проверки за съответствие, независимо дали се извършват вътрешно или от външен консултант, клиент или регулатор

2.2 Настоящата политика се прилага и за събирането на доказателства и докладването за:

2.2.1 Одити за сертификация и ресертификация по ISO/IEC 27001

2.2.2 Одити по защита на данните съгласно GDPR или договорни изисквания

2.2.3 Въпросници по сигурността, инициирани от клиенти, или прегледи в рамките на надлежна проверка

2.2.4 Всички регулаторни или независими прегледи по NIS2 или DORA, когато е приложимо

3. Цели

3.1 Да се гарантира, че всички ключови контроли и политики се преглеждат редовно по отношение на ефективност и съответствие.

3.2 Да се поддържат одитна следа и записи за коригиращи действия с цел демонстриране на отчетност и подобрение.

3.3 Да се осигури подготовка за сертификация, ресертификация и програми за уверение към клиенти (напр. ISO 27001, въвеждане на доставчици).

3.4 Да се идентифицират пропуските на ранен етап, така че да се осигури своевременно отстраняване, преди проблемите да ескалират или да доведат до нарушение на задължения.

3.5 Да се даде възможност на Управителя и Доставчика на ИТ поддръжка да координират прегледите с минимална сложност, като същевременно се гарантират защитими резултати.

4. Роли и отговорности

4.1 Управител

4.1.1 Осъществява надзор върху програмата за одит

4.1.2 Одобрява плановете за вътрешен преглед и констатациите

4.1.3 Възлага и проследява коригиращи действия

4.1.4 Одобрява ангажирането на външни одитори или консултанти

4.2 Доставчик на ИТ поддръжка / администратор

4.2.1 Предоставя доказателства по време на вътрешни и външни одити (напр. журнали, конфигурации, записи за контрол на достъпа)

4.2.2 Съдейства при технически проверки (напр. статус на резервните копия, съответствие при прилагане на корекции)

4.2.3 Поддържа хранилището за одитни доказателства

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

9. Преглед и актуализиране

9.1 Годишен преглед на политиката и плана за одит

9.1.1 Управителят трябва да преглежда тази политика и графика за одит най-малко веднъж годишно.

9.1.2 Прегледът трябва да оценява:

9.1.2.1 Ефективността на одитите при идентифициране на пропуски

9.1.2.2 Процента на завършване на одитите и коригиращите действия

9.1.2.3 Промените в приложимите правни, регулаторни или сертификационни изисквания

9.2 Актуализации, задействани от събитие

9.2.1 Политиката трябва да бъде прегледана и актуализирана, когато:

9.2.2 Одит за сертификация или надзорен одит доведе до съществено несъответствие

9.2.3 Правните или регулаторните рамки се променят (напр. нови указания по GDPR, национално прилагане на NIS2)

9.2.4 Промени в дейността засягат системи, процеси или доставчици, включени в обхвата на одита

9.2.5 Критичен инцидент или нарушение разкрие неидентифицирани преди това пропуски в контролите

9.3 Документиране на актуализациите

9.3.1 Всички редакции трябва да се проследяват в регистър за управление на версиите на политиката

9.3.2 Актуализациите трябва да бъдат разпространявани до всички членове на екипа, участващи в одити

9.3.3 Към актуализираната политика трябва да бъде включено обобщение на промените, за да се гарантира разбиране

10. Свързани политики и връзки

10.1 Настоящата политика се подпомага от и допълва няколко други политики за МСП:

10.1.1 P1S – Политика за информационна сигурност: Определя базовите изисквания към всички контроли и изисква тяхното проверяване чрез одити.

10.1.2 P2S – Политика за роли и отговорности в управлението: Установява отчетност за планирането на одита, изпълнението и собствеността върху коригиращите действия.

10.1.3 P6S – Политика за управление на риска: Идентифицира слабости в контролите, установени при одити, и гарантира, че констатациите се документират в регистъра на риска.

10.1.4 P17S – Политика за защита на данните и поверителност: Определя контролите по GDPR, които подлежат на одит, включително обработване на данни, реагиране при нарушения и уведомления за поверителност.

10.1.5 P22S – Политика за регистриране и мониторинг: Осигурява одитните журнали и форензичните данни, използвани по време на прегледи за съответствие и прегледи на контроли.

10.1.6 P30S – Политика за реагиране при инциденти: Изисква периодичен одит на записите за инциденти и прегледите след събитие с цел проверка на ефективността на реагирането.

10.1.7 P31S – Политика за събиране на доказателства и форензика: Осигурява процедурите за събиране на проверими доказателства и документация за веригата на съхранение по време на одити.

10.2 Заедно тези политики създават затворена контролна среда, която позволява вътрешна верификация, външно уверение и управление, съгласувано със стандартите.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:

11.1.1 Клауза 9.2 – Изисква вътрешен одит за оценка на резултатността на СУИС и съответствието с изискванията.

11.1.2 Клауза 10.1 – Изисква непрекъснато подобрение въз основа на резултатите от одита и отстраняването на несъответствия.

11.2 ISO/IEC 27002:

11.2.1 Контрол 5.35 – Изисква планирани вътрешни прегледи на контролите и процесите.

11.2.2 Контрол 5.37 – Подчертава независимите прегледи, особено за външно възложени процеси.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Оценки на сигурността: Изисква одити на внедрените контроли за проверка на ефективността.

11.3.2 CA-7 – Непрекъснато наблюдение: Подчертава проактивното откриване и прегледа на слабости в контролите.

11.3.3 AU-6 – Преглед, анализ и докладване на одита: Изисква редовен анализ и обработване на одитни журнали и констатации.

11.4 GDPR на ЕС:

11.4.1 Членове 24 и 32 – Изискват внедряване и одитиране на технически и организационни мерки, включително доказателства за ефективността на контролите и подобрение във времето.

11.5 Директива NIS2 на ЕС (2022/2555):

11.5.1 Членове 20–21 – Изискват проактивен преглед на контролите, съответствие, основано на доказателства, и възможност за одитиране за съществени и важни субекти.

11.6 COBIT 2019:

11.6.1 MEA01 – Мониторинг, оценяване и преценка на резултатността и съответствието: Изисква периодична оценка на резултатността на процесите и контролите спрямо стандарти и цели.

11.6.2 MEA03 – Осигуряване на съответствие с външни изисквания: Фокусира се върху вътрешния мониторинг и готовността за одити от трети страни и регулаторни прегледи.