					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P01S					Заглавие на документа: **Политика за информационна сигурност**							
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 регулаторни изисквания

Стандарт/регулация	**Клауза/член**	**Коментар**
ISO/IEC 27001:2022	Клаузи 5.1, 5.2, 5.3, 6.1, 6.2, 8	Определя ангажираността на ръководството, изискванията към политиката, разпределението на ролите, оценката на риска и оперативния контрол
ISO/IEC 27002:2022	Контроли 5.1–5	Определя разработването на документирани политики за информационна сигурност, възлагането на роли, разделението на задълженията и управленските отговорности
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Определя изисквания за план на програмата по сигурност, политика за планиране, оценяване/упълномощаване и контрол на достъпа
EU GDPR (2016/679)	Член 5(2), член 32	Установява принципа на отчетност и мерките за сигурност на обработването, особено по отношение на документираните роли
EU NIS2 Directive (2022/2555)	Член 21(2)(a)	Изисква мерки за управление на риска, както и роли и отговорности по отношение на киберриска
EU DORA (2022/2554)	Член 9, член 10	Изисква разпределяне на роли за управление на ИКТ риска и непрекъсваемост на дейността
COBIT 2019	EDM03, APO13, DSS05	Осигурява оптимизиране на риска, управление на сигурността и управление на услугите по сигурност чрез ясно възлагане на роли

1. Цел

1.1 Настоящата политика отразява ангажимента на организацията към защитата на клиентската и бизнес информация чрез ясно определяне на отговорностите и прилагане на практически мерки за сигурност, подходящи за организации без собствен ИТ екип.

1.2 Тя гарантира, че всички служители, външни изпълнители и доставчици на услуги спазват задължителните правила, което позволява пълно съответствие с изискванията за сертифициране по ISO/IEC 27001.

1.3 Настоящата политика позволява на организацията ясно да демонстрира как защитава информацията на своите клиенти чрез определени отговорности, структурирани процеси и отчетност, като по този начин изгражда доверие у клиентите.

2. Обхват

2.1 Настоящата политика се прилага за всички лица, които имат достъп до данните и системите на организацията или ги управляват, включително:

2.1.1 Собственици на бизнеса и управители

2.1.2 Служители, външни изпълнители и стажанти

2.1.3 Външни доставчици на ИТ услуги или консултанти

2.2 Тя обхваща всички видове информация, системи и услуги, включително:

2.2.1 Бизнес записи, клиентски данни, пароли и електронна поща

2.2.2 ИТ хардуер, като например лаптопи и телефони

2.2.3 Облачни услуги, използвани за съхранение на файлове, комуникация или финансови дейности

2.2.4 Физически документи, съхранявани в офисни помещения

2.3 Политиката се прилага във всички работни среди — в офис, дистанционно и в облачна среда — и обхваща всички устройства и софтуер, използвани за обработване или съхранение на бизнес информация.

3. Цели

3.1 Ясно разпределяне на отговорността: Да се гарантира, че винаги има определено лице, което носи отговорност за информационната сигурност. Обичайно това е Управителят или лице, официално определено от него.

3.2 Защита на клиентската и бизнес информация: Да се осигурят надеждни и последователни защитни мерки за предотвратяване на неправомерно използване, загуба или кражба на чувствителни данни, включително клиентски и финансови записи.

3.3 Подкрепа за сертифициране по ISO/IEC 27001: Да се даде възможност на организацията да демонстрира пълно съответствие с изискванията на ISO/IEC 27001 и готовност за одит, без да е необходима сложна инфраструктура.

3.4 Интегриране на сигурността в бизнес дейността: Да се интегрира информационната сигурност в ежедневните дейности и решения в цялата организация.

3.5 Изграждане на осведоменост и култура по сигурността: Да се насърчава всеки служител да разбира и спазва практиките за сигурност, като използване на силни пароли и докладване на подозрителна дейност.

4. Роли и отговорности

4.1 Управител или собственик на бизнеса

4.1.1 Носи цялостна отговорност за информационната сигурност.

4.1.2 Одобрява и поддържа настоящата политика.

4.1.3 Осигурява изпълнението на всички ключови задачи по сигурността пряко или чрез писмено възлагане.

4.1.4 Проверява дали всички възложени задачи по сигурността, като управление на достъпа или реагиране при инциденти, се изпълняват ефективно.

4.1.5 Изпълнява ролята на основно лице за контакт по всички вътрешни и външни въпроси, свързани със сигурността, включително одити и клиентски запитвания.

4.1.6 Проследява напредъка по тези цели в рамките на годишния преглед. Когато е възможно, целите следва да бъдат измерими, например процент обучен персонал, брой докладвани инциденти и други, и да се актуализират въз основа на констатациите по сигурността и промените в риска.

4.2 Определен служител (ако е приложимо)

4.2.1 Може да подпомага Управителя чрез изпълнение на ежедневни задачи, като създаване на потребителски акаунти, прекратяване на достъп за напускащи служители или координация с ИТ доставчика.

4.2.2 Трябва да бъде официално определен и да разполага с достатъчни правомощия и инструменти за изпълнение на задачите.

4.2.3 Докладва всички проблеми на Управителя.

[... 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 Годишен преглед

9.1.1 Настоящата политика трябва да бъде преглеждана от Управителя най-малко веднъж годишно, за да се осигури текущо съответствие с изискванията за сертифициране по ISO/IEC 27001, промените в регулаторните изисквания, като GDPR, NIS2 и DORA, и развиващите се бизнес потребности.

9.2 Междинни прегледи

9.2.1 Допълнителни прегледи трябва да се извършват винаги, когато има съществени промени, като например:

9.2.1.1 Значими инциденти по сигурността или нарушения

9.2.1.2 Въвеждане на нови бизнес процеси или технологии, например нов софтуер, платформи за дистанционна работа или облачни услуги

9.2.1.3 Промени в правните или регулаторните изисквания, които засягат боравенето с информация

9.3 Документиране на промените

9.3.1 Всички прегледи и промени по политиката трябва да бъдат официално документирани, като ясно се посочват датата, естеството на промените и одобрението на Управителя.

9.3.2 Историята на версиите на политиката трябва да се поддържа сигурно, за да демонстрира развитието на политиката и съответствието при одити.

9.4 Комуникация на актуализациите

9.4.1 Всички промени в настоящата политика трябва своевременно да бъдат съобщавани на всички служители, външни изпълнители и приложими трети страни.

9.4.2 Актуализираните версии на политиката трябва да бъдат лесно достъпни за целия засегнат персонал, например чрез електронно споделяне или физическо публикуване на работното място.

10. Свързани политики и връзки

10.1 Настоящата политика е тясно свързана с други политики от набора политики на организацията за МСП, по-специално:

10.1.1 P2S – Политика за роли и отговорности в управлението: Уточнява възлагането на задължения и отговорности по сигурността.

10.1.2 P4S – Политика за контрол на достъпа: Определя сигурното управление на достъпа до информацията на дружеството.

10.1.3 P8S – Политика за осведоменост и обучение по информационна сигурност: Предоставя основни насоки за обучение и осведоменост на персонала.

10.1.4 P17S – Политика за защита на данните и поверителност: Осигурява съответствие с GDPR и други закони за защита на данните.

10.1.5 P30S – Политика за реагиране при инциденти: Описва подробните действия, които се изискват в отговор на инциденти по сигурността.

10.2 Тези свързани политики предоставят ясни оперативни насоки и трябва да се прилагат съвместно, за да се постигне пълно съответствие с изискванията за сертифициране по ISO/IEC 27001.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 5.1 – Лидерство и ангажираност: Изисква ангажираност на висшето ръководство и отчетност за ефективността на информационната сигурност в рамките на организацията.

11.1.2 Клауза 5.2 – Политика за информационна сигурност: Изисква ясни, документирани политики, съгласувани със стратегията на организацията и изискванията за съответствие.

11.1.3 Клауза 5.3 – Организационни роли и отговорности: Определя ясно възлагане на отговорностите по информационната сигурност в цялата организация, което е съществено за ефективното управление и съответствието при одит.

11.1.4 Клауза 6.1 – Действия за адресиране на рискове и възможности: Осигурява систематично идентифициране, оценяване и третиране на рисковете за информационната сигурност.

11.1.5 Клауза 8.1 – Оперативно планиране и контрол: Изисква организацията да планира и внедрява процесите, необходими за постигане на целите по информационна сигурност и за ефективно управление на свързаните рискове.

11.2 ISO/IEC 27002:2022 Контроли 5.1–5

11.2.1 Приложение A, Контрол 5.1 – Политики за информационна сигурност: Определя създаването и комуникирането на документирани политики за информационна сигурност.

11.2.2 Приложение A, Контрол 5.2 – Роли по информационна сигурност: Уточнява и официално възлага ролите и отговорностите по информационна сигурност на съответните страни.

11.2.3 Приложение A, Контрол 5.3 – Разделение на задълженията: Налага ясно разделение на задълженията, за да се намалят конфликтите на интереси и рисковете от измами при управлението на чувствителна информация.

11.2.4 Приложение A, Контрол 5.4 – Отговорности на ръководството: Изисква ръководството да демонстрира ангажираност към информационната сигурност чрез активен надзор и осигуряване на ресурси.

11.2.5 Подчертава необходимостта от ясно документирани политики, роли, отговорности и структури за управление на информационната сигурност, като гарантира последователно управление и проследимост при одит в цялата организация.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – План на програмата за информационна сигурност: Изисква документирани стратегии и политики за управление на информационната сигурност, които осигуряват рамка за последователно внедряване и управление.

11.3.2 PL-1 – Политика за планиране на сигурността: Изисква политика за планиране на сигурността на организационно ниво, която да насочва сигурната експлоатация и стратегическото съгласуване на дейностите по информационна сигурност.

11.3.3 CA-1 – Политика за оценяване и упълномощаване по сигурността: Изисква ясно определени роли за оценяване и упълномощаване, за да се осигурят постоянна ефективност и съответствие с изискванията за информационна сигурност.

11.3.4 AC-1 – Политика за контрол на достъпа: Изисква организациите ясно да определят, документират и прилагат практиките и отговорностите по управление на достъпа.

11.4 EU GDPR (2016/679)

11.4.1 Член 5(2) – Принцип на отчетност: Изисква организациите да демонстрират съответствие с принципите за защита на данните, включително чрез документирани роли и политики за отговорностите по защита на данните.

11.4.2 Член 32 – Сигурност на обработването: Изисква внедряването на подходящи технически и организационни мерки, включително ясно определени отговорности по сигурността, за защита на личните данни от нарушения и неоторизиран достъп.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Член 21(2)(a) – Мерки за управление на риска: Изисква ясни механизми за управление, включително определени роли и отговорности за информационната сигурност, необходими за ефективно управление на киберрисковете.

11.6 EU DORA (2022/2554)

11.6.1 Член 9 – Управление на ИКТ риска: Изисква организациите ясно да разпределят ролите и отговорностите, свързани с управлението на ИКТ риска, като повишават устойчивостта и готовността за непрекъсваемост на дейността.

11.6.2 Член 10 – Непрекъсваемост на ИКТ дейностите: Изисква ясна отчетност и структурирани роли за поддържане на устойчивостта и непрекъсваемостта на ИКТ, като гарантира, че организациите могат надеждно да реагират при прекъсвания.

11.7 COBIT 2019

11.7.1 EDM03 – Осигуряване на оптимизиране на риска: Подчертава ясно определената отчетност и роли при управлението на организационните рискове, като осигурява стабилно управление и ефективен надзор върху рисковете за информационната сигурност.

11.7.2 APO13 – Управление на сигурността: Изисква организациите ясно да определят и комуникират отговорностите по управление на сигурността, като осигуряват съгласуваност с бизнес целите и регулаторните изисквания.

11.7.3 DSS05 – Управление на услугите по сигурност: Изисква структурирани роли и ясно определени отговорности при управлението на услугите по сигурност, което позволява последователно внедряване и проверка на съответствието.