					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P02S					Заглавие на документа: **Политика за ролите и отговорностите в управлението**							
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 с приложимите стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 5	
ISO/IEC 27002:2022	Мерки: 5.2, 5.3, 5.4	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
GDPR на ЕС	Членове 5(2), 32	

1. Цел

1.1 Настоящата политика определя начина, по който в организацията се възлагат, делегират и управляват отговорностите по управление на информационната сигурност, за да се осигури пълно съответствие с ISO/IEC 27001:2022 и други приложими регулаторни изисквания.

1.2 Тя осигурява отчетност на всички нива и подпомага оперативната ефективност чрез ясно определяне на отговорностите за всяка функция, свързана със сигурността.

1.3 Настоящата политика повишава готовността за одит и изгражда доверие у клиентите, като демонстрира формализирано управление на сигурността, включително в организации с ограничен технически капацитет или с възложени на външни изпълнители ИТ услуги.

2. Обхват

2.1 Настоящата политика се прилага за всички лица, които работят с организационни системи или данни, включително:

2.1.1 собственици на бизнес процеси, управители

2.1.2 служители и външни изпълнители

2.1.3 външни доставчици на ИТ услуги или консултанти

2.2 Тя обхваща всички системи, среди и услуги, използвани за обработване, предаване или съхранение на служебна или клиентска информация, включително:

2.2.1 офис ИТ инфраструктура и устройства за дистанционна работа

2.2.2 облачни платформи и услуги за електронна поща

2.2.3 физически записи и споделени мрежови устройства

2.3 Обхватът включва както вътрешни дейности, така и дейности, възложени на външни изпълнители, свързани с управлението на информационната сигурност.

3. Цели

3.1 Да се установи ясна отчетност за всички задължения, свързани със сигурността, включително управление на политики, контрол на достъпа, обработване на инциденти и мониторинг.

3.2 Да се осигури ефективно разделение на задълженията с цел намаляване на конфликти на интереси или риск от измами.

3.3 Да се гарантира, че задачите и ролите по сигурността са ясно документирани и се преглеждат регулярно.

3.4 Да се осигури информирано вземане на решения, ескалация и надзор върху ИТ рисковете и рисковете за сигурността.

3.5 Да се подпомогне сертифицирането по ISO/IEC 27001:2022 и да се изгради доверие сред клиенти, партньори и одитори.

4. Роли и отговорности

4.1 Управител / собственик на бизнеса

4.1.1 Носи цялостна отговорност за внедряването и надзора върху прилагането на настоящата политика.

4.1.2 Одобрява всички роли, отговорности и решения за делегиране, свързани със сигурността.

4.1.3 Следи съответствието и взема окончателни решения по изключения от политиката и ескалации.

4.2 Определен координатор по сигурността (ако е назначен)

4.2.1 Може да бъде служител или доверен консултант.

4.2.2 В среда на микропредприятие тази роля може да се изпълнява от управителя или от външен доставчик.

4.2.3 Подпомага ежедневното прилагане на контрола на достъпа, реагирането при инциденти и основни технически дейности по сигурността.

4.2.4 Докладва пряко на управителя за всички въпроси или рискове, свързани със сигурността.

[... 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 Ежегоден преглед

9.1.1 Настоящата политика трябва да бъде преглеждана от управителя на всеки 12 месеца, за да се гарантира, че продължава да отразява правните задължения, оперативните потребности и изискванията за сертифициране по ISO/IEC 27001.

9.2 Междинни прегледи

9.2.1 Прегледи трябва да се извършват и когато:

9.2.1.1 има съществени организационни промени

9.2.1.2 бъде въведен нов доставчик

9.2.1.3 възникне сериозен инцидент по сигурността

9.2.1.4 регулации като GDPR, NIS2 или DORA бъдат актуализирани

9.3 Управление на версиите и документация

9.3.1 Всички прегледи трябва да включват:

9.3.1.1 дата на прегледа

9.3.1.2 обобщение на всички промени

9.3.1.3 подпис или документирано одобрение от управителя

9.3.1.4 архивирани предходни версии за целите на одита

9.4 Комуникиране на промените

9.4.1 Всички актуализации на политиката трябва своевременно да бъдат съобщавани на персонала и доставчиците чрез електронна поща, вътрешни портали или официални служебни съобщения.

10. Свързани политики и връзки

10.1 Настоящата политика следва да се прилага съвместно със следните SME политики за пълна ефективност:

10.1.1 P4S – Политика за контрол на достъпа: определя как се предоставя, управлява и отнема достъпът и е пряко свързана с възложените роли и надзора.

10.1.2 P8S – Политика за осведоменост и обучение по информационна сигурност: утвърждава специфичните за ролята отговорности и очаквания.

10.1.3 P17S – Политика за защита на данните и поверителност: определя правните задължения по GDPR, които се възлагат на ролите, определени в настоящата политика за управление.

10.1.4 P30S – Политика за реагиране при инциденти: изисква ясно определени отговорности за докладване, ескалация и разрешаване на инциденти.

10.2 Заедно тези политики осигуряват последователно прилагане, вътрешна отчетност и външно съответствие.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 5.3 – Организационни роли, отговорности и правомощия: изисква ролите да бъдат ясно възложени и подкрепени от висшето ръководство.

11.2 ISO/IEC 27002

11.2.1 Мерки 5.2–5.4: изискват ясно документиране на ролите по информационна сигурност, разделение на задълженията и управленски надзор.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: установява обща програма по информационна сигурност с определени отговорности.

11.3.2 PL-1 до PL-4: изискват мерки за планиране, включително формулиране на политики и документирано възлагане на роли.

11.3.3 CA-1: изисква определени роли за оценяване и оторизиране.

11.3.4 AC-1: обвързва ролевия контрол на достъпа (RBAC) с възложените отговорности по управление.

11.4 GDPR на ЕС

11.4.1 Член 5(2) – Отчетност: изисква организациите да демонстрират съответствие чрез роли и отговорности.

11.4.2 Член 32 – Сигурност на обработването: подчертава необходимостта от ясно възлагане на задължения за защита на личните данни.

11.5 Директива NIS на ЕС

11.5.1 Член 21(2)(a): изисква структури за управление, които включват формализирани роли за управление на киберриска и инцидентите.

11.6 DORA на ЕС

11.6.1 Членове 9 и 10: изискват финансовите субекти ясно да възлагат и упражняват надзор върху отговорностите, свързани с ИКТ и сигурността.

11.7 COBIT 2019

11.7.1 EDM03 – Осигуряване на оптимизация на риска: изисква добре дефинирани роли и маршрути за ескалация при управлението на риска за сигурността.

11.7.2 APO13 – Управление на сигурността: възлага стратегически и оперативни задължения по сигурността на конкретни лица и роли.

11.7.3 DSS05 – Управление на услугите по сигурност: изисква структура и проследимост на отговорностите за външни и вътрешни услуги по сигурност.