					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P02					Заглавие на документа: **Политика за ролите и отговорностите по 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**

Съгласуваност с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 5.3; Контрол 5 от Приложение A	
ISO/IEC 27002:2022	Контрол 5	
NIST SP 800-53 Rev.5	PL-1 до PL-4, PM-1 до PM-13	
GDPR на ЕС	Членове 5(1)(f), 24, 37	
NIS2 на ЕС	Член 21(2)(a)	
DORA на ЕС	Член 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Цел

1.1 Настоящата политика определя модела на управление, организационните роли и отговорностите, необходими за функционирането на ефективна Система за управление на информационната сигурност (ISMS).

1.2 Политиката установява ясни линии на отчетност, правомощия за вземане на решения и канали за ескалация, за да гарантира, че информационната сигурност е интегрирана на всички нива в организацията и съгласувана със стратегическите бизнес цели.

1.3 Политиката прилага изискванията на ISO/IEC 27001:2022, Клауза 5.3 и Контрол A.5.2, като гарантира, че отговорностите за дейностите, свързани със сигурността, са ясно определени, документирани, комуникирани и периодично преглеждани.

1.4 Настоящата политика също така осигурява основа за интегрирано управление с други области, като управление на риска, съответствие, ИТ операции и правни функции.

2. Обхват

2.1 Настоящата политика се прилага за всички лица и звена, участващи в управлението, изпълнението и надзора на информационната сигурност в обхвата на ISMS. Това включва:

2.1.1 висшето ръководство, старшия мениджмънт и членовете на управителния орган

2.1.2 мениджърите на ISMS, CISO и притежателите на контроли

2.1.3 собствениците на процеси и активи

2.1.4 изпълнителите по договор и външните доставчици на услуги с делегирани отговорности по сигурността

2.2 Политиката обхваща както вътрешни, така и външно предоставяни функции (напр. външен SOC, администратори на облачни платформи), когато ролите по управление са формално възложени или договорно определени.

2.3 Политиката се прилага и за организационни единици, отдели и проектни екипи, които управляват или оказват влияние върху активи, системи или услуги, имащи отношение към сигурността.

3. Цели

3.1 Да се гарантира, че ролите и отговорностите по информационна сигурност са формално определени, възложени, комуникирани и документирани.

3.2 Да се поддържа модел на управление, който осигурява разделение на задълженията, предотвратява конфликти на интереси и позволява ескалация на нерешени въпроси, свързани със сигурността.

3.3 Да се гарантира, че отчетността и правомощията за вземане на решения по сигурността са разпределени в съответствие с бизнес въздействието и организационната структура.

3.4 Да се установи рамка за управление на делегирането, промените в ролите и прегледа на възложените отговорности.

3.5 Да се предостави увереност на заинтересованите страни, включително регулатори, одитори и клиенти, че информационната сигурност се управлява ефективно и в съответствие с приложимите стандарти.

4. Роли и отговорности

4.1 Изпълнително ръководство (висше ръководство)

4.1.1 Осигурява стратегически надзор, разпределя ресурси и гарантира съгласуваност между целите на ISMS и бизнес целите.

4.1.2 Одобрява основната документация по ISMS, включително Политиката за информационна сигурност, плановете за третиране на риска и решенията за отстраняване на одитни несъответствия.

4.1.3 Участва в прегледите на ISMS от ръководството и ескалира решенията, изискващи одобрение на ниво управителен орган.

4.1.4 Насърчава култура на сигурност и подпомага спазването в организацията на принципите за управление на сигурността.

4.2 Комитет по управление на информационната сигурност (ISSC)

4.2.1 Изпълнява ролята на междуфункционален орган за управление, осъществяващ надзор върху ISMS.

4.2.2 Преглежда профила на риска, ефективността на контролите, одитните констатации и стратегическите инициативи по сигурността.

4.2.3 Подпомага координацията между отделите (напр. ИТ, Правен, Човешки ресурси, Риск, Съответствие, Операции).

4.2.4 Одобрява праговете за ескалация, разпределението на бюджетите и промените в политики, изискващи участие на изпълнителното ръководство.

[... 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 График за преглед

9.1.1 Настоящата политика се преглежда най-малко веднъж годишно или при настъпване на:

9.1.1.1 промени в организационната структура или в състава на изпълнителното ръководство

9.1.1.2 разширяване или предефиниране на обхвата на ISMS

9.1.1.3 регулаторни промени, засягащи възлагането на роли или надзора

9.1.1.4 съществени одитни констатации или инциденти, свързани с пропуски в управлението

9.2 Процес по преглед и одобрение

9.2.1 Мениджърът на ISMS инициира и ръководи процеса по преглед, включително събиране на мнения от заинтересованите страни и обратна връзка от одитите.

9.2.2 Предложените актуализации се преглеждат от ISSC и се одобряват формално от изпълнителното ръководство.

9.2.3 Всяка версия трябва да бъде проследявана в Регистъра на документите на ISMS и да включва следните метаданни:

9.2.3.1 идентификатор и заглавие на политиката

9.2.3.2 номер на версията и обобщение на промените

9.2.3.3 дата на влизане в сила и дата на следващия преглед

9.2.3.4 собственик на политиката и одобряващ

9.2.3.5 ниво на класификация на документа

9.2.3.6 срок за съхранение и история на архивиране

10. Свързани политики и връзки

10.1 Настоящата политика следва да се тълкува съвместно със следните политики:

10.1.1 P1 – Политика за информационна сигурност: установява цялостната програма по сигурност и определя отговорностите на ръководството за утвърждаване на политиката и стратегически надзор.

10.1.2 P5 – Политика за управление на промените: гарантира, че промените в структурите за управление, ролите или отговорностите подлежат на документирано одобрение и преглед на риска.

10.1.3 P6 – Политика за управление на риска: идентифицира и третира рисковете, свързани с управлението, произтичащи от конфликти между роли, невъзложени задължения или липса на ескалация.

10.1.4 P7 – Политика за назначаване и прекратяване: прилага процеси за предоставяне и отнемане на контроли при промени в жизнения цикъл на персонала.

10.1.5 P33 – Политика за одит и наблюдение на съответствието: подпомага независимия преглед на ефективността на управлението и осигурява изпълнение на коригиращи действия при несъответствие.

10.2 Тези политики съвместно поддържат единна и приложима рамка за управление на ISMS.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати стандарти и рамки за управление на информационната сигурност и отчетност по роли. Тя осигурява проследимост към регулаторните изисквания и изискванията за сертифициране и подпомага защитима структура на ISMS.

11.2 ISO/IEC 27001

11.2.1 Клауза 5.3 – Организационни роли, отговорности и правомощия: настоящата политика изпълнява изискването ролите, свързани с информационната сигурност, да бъдат ясно възложени, комуникирани и документирани.

11.2.2 Клауза 9.3 – Преглед от ръководството: настоящата политика осигурява надзор от изпълнителното ръководство върху ролите и управлението на ISMS чрез тримесечни и годишни прегледи.

11.2.3 Контрол 5.2 от Приложение A – Роли и отговорности по информационна сигурност: определя роли на техническо, оперативно и стратегическо ниво, за да осигури разделение на задълженията, притежание на риска и проследима отчетност.

11.3 ISO/IEC 27002:2022 – Контрол 5

11.3.1 Предоставя указания за прилагане относно възлагането на отговорности по информационна сигурност в рамките на организацията. Настоящата политика възприема

тези указания чрез определяне на типове роли, правила за делегиране, процедури за ескалация и механизми за преглед.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 до PL-4: налагат необходимостта от формализирана документация за планиране, включително политики, които определят управлението и възлагат отговорности по сигурността.

11.4.2 PM-1 (План на програмата по информационна сигурност) и PM-2 (Старши служител по информационна сигурност): отразени са в настоящата политика чрез определянето на CISO/Мениджъра на ISMS и формални роли по управление.

11.4.3 PM-5 до PM-13: настоящата политика покрива изискванията за документиране на роли, роли по управление на риска в цялата организация, надзор върху управлението на конфигурациите и интеграция с основните бизнес функции.

11.5 GDPR на ЕС (2016/679)

11.5.1 Член 5(1)(f): изисква личните данни да бъдат защитени срещу неразрешено или незаконосъобразно обработване. Настоящата политика гарантира, че лицата, отговорни за защитата на данните, са ясно определени и подлежат на надзор.

11.5.2 Член 24: изисква подходящи организационни мерки, включително структури за управление.

11.5.3 Член 37: изисква определяне на длъжностно лице по защита на данните (DPO), което трябва да бъде отразено в рамката за управление на организацията и в регистъра на отговорностите.

11.6 Директива NIS2 на ЕС (2022/2555)

11.6.1 Член 21(2)(a): изисква организациите да прилагат политики за анализ на риска и сигурността на информационните системи, включително отговорности, специфични за ролите. Настоящата политика определя такива роли и механизмите за тяхното управление.

11.7 DORA на ЕС (2022/2554)

11.7.1 Член 5 – Рамка за управление и вътрешен контрол: изисква формално възлагане на отговорности по управление на ИКТ риска, роли за вземане на решения и канали за докладване. Настоящата политика осигурява основата за управление на ролите, свързани със сигурността, в ИКТ среда.

11.8 COBIT 2019

11.8.1 EDM01 – Осигуряване на рамката за управление: настоящата политика гарантира, че ISMS разполага с ясно определена структура за управление, съгласувана с нуждите на организацията.

11.8.2 EDM02 – Осигуряване на предоставянето на ползи: съгласува дейностите по сигурност, базирани на роли, със стратегическите и оперативните цели, като осигурява отчетност и измерими резултати.

11.8.3 APO01 – Управлявана рамка за управление на I&T и APO12 – Управляван риск: настоящата политика подпомага структурираното управление на ролите по информационна сигурност в рамките на по-широка рамка за ИТ управление и управление на риска.

11.8.4 MEA01 – Наблюдение, оценяване и преценка на ефективността: въвежда механизми за преглед с цел потвърждение, че ролите по управление са ефективни, актуални и се прилагат.