					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P06					Заглавие на документа: **Политика за управление на риска**							
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**

Съгласувана с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1, 8.32, 10	Основа за идентифициране и управление на риска, интегриране в управлението на промените, непрекъснато подобрение
ISO/IEC 27005:2024	Пълна методология за жизнения цикъл на риска	Цялостен процес по управление на риска в съответствие със стандарта
ISO 31000:2018	Принципи и рамка за управление на риска	Принципите за управление на риска са възприети в рамката
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Насоки и структура за оценка на риска, многостепенно управление на риска
EU GDPR	Членове 24, 25, 32	Процеси и контроли за риска, свързан със защитата на данните
EU NIS2	Член 21(2)(a–d)	Задължения за оценка на риска и сигурността
EU DORA	Членове 5, 6	Управление на ИКТ риска и оперативна устойчивост
COBIT 2019	APO12, MEA	Структура за управление на риска и надзор

1. Цел

1.1 Настоящата политика установява единна и формализирана рамка за идентифициране, анализ, оценяване, третиране, мониторинг и преглед на рисковете за информационната сигурност в цялата организация.

1.2 Политиката осигурява последователно прилагане на принципи, основани на риска, които защитават поверителността, целостта и наличността (CIA) на информационните активи, в съответствие с Клауза 6.1 на ISO/IEC 27001:2022 и ISO 31000:2018.

1.3 Политиката интегрира управлението на риска за информационната сигурност в процесите по вземане на решения в организацията с цел изпълнение на вътрешните стратегически цели и външните регулаторни изисквания.

2. Обхват

2.1 Настоящата политика се прилага за всички организационни единици, бизнес процеси, системи, персонал и ангажименти с външни изпълнители, свързани с обработването, разработването, съхранението или управлението на информационни активи.

2.2 Обхватът включва физически, цифрови и облачно хоствани активи, включително структурирани и неструктурирани данни, приложения, инфраструктура, мрежи и услуги.

2.3 Политиката обхваща рисковете за информационната сигурност на стратегическо, оперативно, проектно и техническо ниво и е задължителна за всички служители, външни изпълнители и доставчици на услуги, ангажирани с дейности по СУИС.

2.4 Управлението на риска се прилага в следните сценарии:

2.4.1 внедряване на нов проект или система

2.4.1.1 значими промени (напр. архитектура, собственост, процеси)

2.4.1.2 въвеждане на доставчици и сключване на споразумения с трети страни

2.4.1.3 реагиране при инциденти и прегледи след инцидент

2.4.1.4 периодични организационни прегледи на риска или одити

3. Цели

3.1 Да се установи и въведе в действие повтаряем, приложим в цялата организация процес по управление на риска, базиран на методологиите на ISO/IEC 27005 и ISO 31000.

3.2 Да се гарантира, че рисковете се идентифицират, анализират, оценяват и третират чрез структурирани и проследими методи, включително чрез определяне на собствеността върху риска и връзките с контроли.

3.3 Да се поддържат централизиран регистър на риска и планове за третиране на риска с управление на версиите, които отразяват текущия статус на риска, покритието на контролите и напредъка по смекчаването.

3.4 Да се съгласуват решенията относно риска с документирания апетит към риска и нивата на толерантност към риска и да се подпомогне информираното управленско вземане на решения относно приемане, смекчаване, прехвърляне или избягване на риска.

3.5 Да се осъществява непрекъснат мониторинг на тенденциите при риска и да се гарантира ефективността на третирането на риска, като същевременно се осигурява проактивно адаптиране спрямо развитието на заплахите или промените в бизнеса.

4. Роли и отговорности

4.1 Изпълнително ръководство / Съвет на директорите

4.1.1 Одобрява рамката за управление на риска и определя приемливия апетит към риска и праговете на толерантност към риска.

4.1.2 Одобрява стратегии за третиране на риска при остатъчна експозиция, която надвишава толерантността.

4.1.3 Осигурява ресурси и надзор за ефективното функциониране на програмата за управление на риска.

4.2 Мениджър на СУИС / Длъжностно лице по управление на риска

4.2.1 Отговаря за настоящата политика и поддържа съответствието ѝ със стандартите ISO/IEC 27001 и ISO/IEC 27005.

4.2.2 Ръководи процеса по оценка на риска в организацията и поддържа регистъра на риска и плановете за третиране на риска.

4.2.3 Осигурява периодични прегледи и ескалация на ключовите рискове към изпълнителното ръководство или ръководния комитет по СУИС.

[... 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 и свързаната с нея рамка трябва да се преглеждат ежегодно или:

9.1.1 след значимо рисково събитие или инцидент по сигурността

9.1.2 след значима организационна или техническа промяна

9.1.3 в отговор на констатации от одит или нови регулаторни изисквания

9.2 Мениджърът на СУИС, длъжностното лице по управление на риска и екипът по съответствие носят съвместна отговорност за:

9.2.1 иницииране на цикъла по преглед

9.2.2 събиране на входна информация от бизнес звената

9.2.3 преразглеждане на процедурите и праговете при необходимост

9.3 Всички изменения трябва да бъдат:

9.3.1 под управление на версиите и регистрирани

9.3.2 одобрени от изпълнителното ръководство

9.3.3 комуникирани до заинтересованите страни

9.3.4 съхранявани в одитното хранилище за минимум 5 години

10. Свързани политики и връзки

10.1 Настоящата политика е взаимосвързана със следните политики по информационна сигурност:

10.1.1 P1 – Политика за информационна сигурност: Определя общия модел за управление на сигурността, в рамките на който се прилага настоящата политика за риска.

10.1.2 P2 – Политика за роли и отговорности в управлението: Определя отговорните собственици и управленските нива, посочени в матрицата за ескалация на риска.

10.1.3 P5 – Политика за управление на промените: Инициира повторна оценка на риска при промени в инфраструктурата и организацията.

10.1.4 P13 – Политика за класификация и етикетиране на данни: Подпомага оценката на въздействието по време на идентифицирането на риска.

10.1.5 P33 – Политика за мониторинг на одита и съответствието: Валидира спазването на политиката, включително пълнотата на регистъра на риска и доказателствата за изпълненото третиране.

11. Референтни стандарти и рамки

11.1 Настоящата политика е изрично съгласувана със следните стандарти и рамки, за да гарантира съответствие с международните добри практики и регулаторните очаквания за управлението на риска за информационната сигурност:

11.2 ISO/IEC 27001:

11.2.1 Клауза 6.1: Установява изискванията за идентифициране на рискове и възможности, включително пълния жизнен цикъл на оценките и третирането на риска за информационната сигурност. Настоящата политика прилага на практика Клауза 6.1.2 и 6.1 чрез структурирана рамка, която изисква документирани протоколи за идентифициране, анализ, оценка, третиране и приемане на остатъчния риск.

11.2.2 Клауза 8.32: Интегрирането на мислене, основано на риска, в процесите по управление на промените гарантира, че всички съществени организационни промени водят до формални повторни оценки на риска.

11.2.3 Клауза 10: Непрекъснатото подобрение е заложено чрез редовни прегледи на политиката, анализ на тенденциите при риска и актуализации на SoA, основани на резултатите от управлението на риска.

11.3 ISO/IEC 27005:

11.3.1 Предоставя специализирани и подробни насоки за управлението на риска за информационната сигурност. Настоящата политика прилага пълния процесен модел на ISO/IEC 27005 за риска: определяне на контекста, идентифициране на риска, анализ на

риска, оценка на риска, третиране на риска, приемане на риска, комуникация на риска, мониторинг и преглед на риска.

11.4 ISO 31000:

11.4.1 Настоящата политика интегрира принципите на ISO 31000, като ангажираност на ръководството, интеграция с процесите по вземане на решения и непрекъснато подобрение. Тя гарантира, че управлението на риска е вградено в културата и дейността на организацията.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Съответства на ръководството на NIST за извършване на оценки на риска, включително идентифициране на заплахи, анализ на уязвимости, оценка на вероятността и определяне на въздействието. Структурата на настоящата политика отразява определените от NIST стъпки за оценка на риска и ги адаптира както за технически, така и за бизнес процеси.

11.6 NIST SP 800-39:

11.6.1 Подпомага управлението на риска на организационно ниво, като акцентира върху многостепенното управление на риска на ниво организация, мисия/бизнес процес и информационна система. Политиката гарантира, че собствеността върху риска е ясно определена на всички нива и включва стратегии за третиране на организационно ниво.

11.7 EU GDPR:

11.7.1 Член 24: Изисква прилагането на подходящи технически и организационни мерки, за да се гарантира, че рисковете, свързани със защитата на данните, се управляват по подходящ начин — разгледано чрез структурирания процес по управление на риска в настоящата политика.

11.7.2 Член 25: „Защита на данните още при проектирането и по подразбиране“ съответства на интегрирането на третирането на риска в проектите на системи и процеси.

11.7.3 Член 32: Изисква основан на риска подход към мерките за сигурност — изпълнен чрез оценки на риска, базирани на въздействието, и избор на контроли.

11.8 Директива EU NIS2:

11.8.1 Член 21(2)(a–d): Изисква организациите да извършват оценки на риска, да прилагат политики за анализ на риска и да осигуряват пропорционални мерки за сигурност. Настоящата политика изпълнява тези задължения чрез непрекъснато прилагане на жизнения цикъл на риска и документирано управление.

11.9 EU DORA:

11.9.1 Член 5: Изисква документирана рамка за управление на ИКТ риска — изцяло обхванатата от архитектурата на настоящата политика, включително съпоставяне със SoA и ключови индикатори за риска.

11.9.2 Член 6: Изисква интегриране на управлението на риска в стратегиите за оперативна устойчивост, разгледано чрез матрици за ескалация и проследяване на критични активи.

11.10 COBIT 2019:

11.10.1 APO12 – Управление на риска: Пряко съответства на установения в организацията структуриран подход за управление на риска, включително определяне на роли, проследяване на третирането и осигуряване на отчетност на ниво Съвет на директорите.

11.10.2 MEA01 – Мониторинг, оценяване и преценка на резултатността и съответствието: Отразен е във фокуса на настоящата политика върху анализа на тенденциите, мониторинга на ключови индикатори за риска и интегрирането на обратната връзка от одита в циклите на непрекъснато подобрение.