					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P06S					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, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 до RA-7, PM-9	
EU NIS2	Член 21(2)(a–d)	
EU DORA	Член 5	
COBIT 2019	APO12, MEA01	

1. Цел

1.1 Тази политика определя как организацията идентифицира, оценява и управлява рисковете, свързани с информационната сигурност, дейността, технологиите и услугите, предоставяни от трети страни.

1.2 Тя гарантира, че управлението на риска е неразделна част от планирането, изпълнението на проекти, избора на доставчици и реагирането при инциденти, в съответствие с ISO 27001, ISO 31000 и приложимите регулаторни изисквания.

1.3 Политиката подпомага вземането на информирани решения, защитата на информационните активи и устойчивостта на критичните бизнес операции.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 Всички отдели, системи и потребители в рамките на организацията

2.1.2 Цялата информация, услуги и активи, управлявани вътрешно или чрез трети страни

2.1.3 Дейности, свързани с риска, включително прегледи на проекти, надграждане на системи, възлагане на външни услуги и регулаторно съответствие

2.2 Тя обхваща всички видове рискове, включително:

2.2.1 Заплахи за киберсигурността и уязвимости на системите

2.2.2 Оперативни прекъсвания и недостъпност на услуги

2.2.3 Правни рискове, рискове по съответствието и репутационни експозиции

2.2.4 Рискове, свързани с трети страни и веригата на доставки

2.3 Всички служители, външни изпълнители и доставчици на услуги са длъжни да спазват тази политика при идентифициране или докладване на рискове.

3. Цели

3.1 Да интегрира прости и повторяеми процедури за оценка на риска в обичайната бизнес дейност.

3.2 Да идентифицира и приоритизира рисковете, които могат да повлияят на поверителността, целостта, наличността или правното съответствие.

3.3 Да определи собственик на риска и действия за третиране на всички съществени рискове.

3.4 Да поддържа точен и актуален Регистър на риска в подкрепа на готовността за одит и проследимостта на риска.

3.5 Да осигурява участието на ръководството при одобряване на толеранса към риска и основните планове за третиране на риска.

4. Роли и отговорности

4.1 Управител

4.1.1 Определя апетита към риска на организацията и утвърждава рамката за управление на риска.

4.1.2 Одобрява основните решения за третиране на риска и необходимите ресурси.

4.1.3 Преглежда най-значимите рискове на тримесечна база съвместно с Координатора по риска.

4.2 Координатор по риска (или Собственик на СУИС)

4.2.1 Подпомага провеждането на оценки на риска и поддържа Регистъра на риска.

4.2.2 Осигурява документирането на оценката на риска, собствеността на риска и действията за отстраняване.

4.2.3 Организира най-малко един формален преглед на риска годишно.

[... 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 Ежегоден преглед на политиката

9.1.1 Тази политика трябва да се преглежда най-малко веднъж годишно от Управителя и Координатора по риска, за да се гарантират нейната приложимост и пълнота.

9.2 Основания за актуализация

9.2.1 По-ранен преглед и актуализация трябва да се извършат, ако:

9.2.1.1 Съществен инцидент или одитна констатация разкрие пропуски в управлението на риска

9.2.1.2 Бъдат въведени нови бизнес единици, технологии или партньорства

9.2.1.3 Има промяна в регулаторно или договорно изискване

9.3 Управление на версиите

9.3.1 Всички актуализации на тази политика трябва да се поддържат с версии със следните метаданни:

9.3.1.1 Номер на версията и дата на влизане в сила

9.3.1.2 Обобщение на промените

9.3.1.3 Одобряващ (Управител)

9.3.1.4 Архивирани предходни версии за целите на одита

9.4 Комуникация и осведоменост

9.4.1 Актуализираните версии на политиката и основните планове за третиране на риска трябва да бъдат комуникирани на засегнатия персонал. Ежегодното обучение за осведоменост трябва да включва основни принципи за осведоменост относно риска.

10. Свързани политики и взаимовръзки

10.1 Тази политика се прилага в координация с няколко други политики, за да се осигури цялостно управление на сигурността:

10.1.1 P2S – Политика за роли и отговорности в управлението: Определя кой носи отговорност за собствеността на риска и вземането на решения.

10.1.2 P5S – Политика за управление на промените: Изисква оценка на риска преди внедряване на технически или процесни промени.

10.1.3 P17S – Политика за защита на данните и поверителност: Разглежда регулаторния риск, свързан с обработването на лични данни.

10.1.4 P30S – Политика за реагиране при инциденти: Осигурява продължаване на третирането на риска по време на и след инциденти по сигурността.

10.1.5 P33S – Политика за непрекъсваемост на дейността: Идентифицира остатъчните рискове и мерките за възстановяване за критични услуги.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:

11.1.1 Клауза 6.1 – Установява формален процес за управление на риска и планиране на третирането.

11.1.2 Клауза 6.1.3 – Изисква организациите да поддържат документирани планове за третиране и одобрения.

11.2 ISO/IEC 27002:

11.2.1 Контроли 5.4, 5.25 – Предоставят насоки за внедряване относно собствеността на риска, приоритизирането и управлението на жизнения цикъл.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 до RA-7 – Определят оценката на риска, стратегиите за реагиране, документирането и механизмите за преглед.

11.4 PM-9 – Изисква последователен надзор на организационните рискове на управленско ниво.

11.5 Директива на ЕС NIS2

11.5.1 Член 21(2)(a–d) – Налага задължителни контроли за оценка на риска, смекчаване и управление за съществени и важни субекти.

11.6 EU DORA

11.6.1 Член 5 – Изисква регулираните субекти да определят и управляват рамки за управление на ИКТ риска, включително идентификация, класификация и реагиране.

11.7 COBIT 2019

11.7.1 APO12 – Управление на риска: Интегрира риска в стратегическото и оперативното планиране.

11.7.2 MEA01 – Мониторинг, оценяване и преценка: Осигурява ефективност и съответствие на процесите и действията по риска.