					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P33					Заглавие на документа: **Политика за одит и мониторинг на съответствието**							
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 със стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 9.2, 9.3, 10	
ISO/IEC 27002:2022	Контроли 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
GDPR на ЕС	Членове 24, 32, 33	
NIS2 на ЕС	Член 21(2)(g), 27	
DORA на ЕС	Членове 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Цел

1.1 Целта на тази политика е да установи и регламентира програмата на организацията за одит и мониторинг на съответствието, така че да:

1.1.1 валидира ефективността на контролите за сигурност и поверителност

1.1.2 осигурява съответствие с приложимите стандарти, нормативни изисквания и договорни задължения

1.1.3 установява своевременно несъответствия, неефективности и рискове, свързани със съответствието

1.1.4 подпомага непрекъснатото подобрение и готовността за сертифициране, оценки и регулаторни прегледи

1.2 Тази политика подпомага целостта и зрелостта на Системата за управление на информационната сигурност (СУИС), като въвежда структурирани, основани на риска и базирани на доказателства практики за одит и мониторинг.

2. Обхват

2.1 Тази политика се прилага за:

2.1.1 всички вътрешни бизнес звена, функции и отдели

2.1.2 физически обекти, облачни среди, SaaS платформи и възложени на външни изпълнители услуги

2.1.3 информационни системи, приложения, инфраструктура и информационни активи, управлявани в рамките на СУИС

2.1.4 служители, външни изпълнители и външни доставчици на услуги, които имат задължения, свързани с одит или съответствие

2.2 Политиката обхваща:

2.2.1 вътрешен одит

2.2.2 външни/сертификационни одити

2.2.3 технически мониторинг на съответствието

2.2.4 одити на доставчици и трети страни

2.2.5 коригиращи и превантивни действия (CAPA)

2.2.6 показатели, информационни табла и процеси по докладване

2.3 Тя се прилага за всички приложими рамки, на които организацията подлежи, включително ISO/IEC 27001, GDPR, NIS2, DORA и SOC 2, наред с други.

3. Цели

3.1 Да се проверяват адекватността и ефективността на внедрените контроли, политики и процедури в рамките на СУИС и свързаните среди.

3.2 Да се идентифицират и отстраняват всички дефицити в контролите, несъответствия или пропуски в съответствието, преди да ескалират до инциденти или нарушения.

3.3 Да се осигурява устойчива готовност за вътрешни прегледи от ръководството, външни одити и независими сертификации.

3.4 Да се създават доказателства с достатъчна правна стойност и одитна следа в подкрепа на регулаторни запитвания, съдебни производства или искания от клиенти за потвърждение на контролите.

3.5 Да се интегрират резултатите от одитите в по-широките дейности на организацията по управление на риска, показателите за сигурност и непрекъснатото подобрение.

4. Роли и отговорности

4.1 Ръководител на вътрешния одит / Мениджър по съответствието

4.1.1 Планира, графицира и изпълнява вътрешния одит въз основа на рисковите приоритети.

4.1.2 Поддържа одитен регистър, координира дейностите по одит и проследява коригиращите действия.

4.2 Директор по информационна сигурност (CISO)

4.2.1 Осигурява обхватът на одита да включва всички приложими елементи на СУИС и контролите от Приложение А.

4.2.2 Упражнява надзор върху верифицирането на CAPA и интегрира резултатите от одитите в програмата по сигурност.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Преглед и актуализиране на изискванията

9.1 Тази политика трябва да бъде преглеждана най-малко веднъж годишно от Мениджъра по съответствието и Директора по информационна сигурност (CISO), или по-рано в отговор на:

9.1.1 промени в регулаторните, договорните или сертификационните рамки

9.1.2 съществени одитни констатации или повтарящи се откази на контроли

9.1.3 организационно преструктуриране или промени в GRC системата

9.1.4 препоръки от външни одитори или обратна връзка от регулатор

9.2 Процесът по преглед трябва да оценява:

9.2.1 методологията и честотата на планиране на одитите

9.2.2 промени в обхвата на СУИС или инфраструктурата

9.2.3 актуализации на каталога с контроли или правния регистър

9.2.4 последователността и качеството на доказателствата за одит и процесите по CAPA

9.3 Всички промени в политиката трябва да бъдат:

9.3.1 документирани в хранилище под управление на версиите

9.3.2 одобрени от Изпълнителното ръководство

9.3.3 комуникирани до целия засегнат персонал и интегрирани в актуализирани процедури и програми за осведоменост

9.4 Валидирането след прегледа трябва да потвърди, че актуализираните изисквания са отразени в одитния регистър, инструментите за съответствие и вътрешните информационни табла за мониторинг.

10. Свързани политики и връзки

10.1 Тази политика е съгласувана със следните свързани организационни политики:

10.1.1 P1 – Политика за информационна сигурност: определя СУИС и установява отчетност за съответствието и непрекъснатото подобрение

10.1.2 P5 – Политика за управление на промените: осигурява видимост при одит върху промените в инфраструктурата и конфигурацията, засягащи контролната среда

10.1.3 P6 – Политика за управление на риска: интегрира резултатите от одитите в дейностите по оценка и третиране на риска в цялата организация

10.1.4 P14 – Политика за съхранение на данни и унищожаване: урежда съхранението на доказателства за одит, журнали и записи по съответствие

10.1.5 P18 – Политика за криптографски контроли: подпомага сигурното съхранение и пренос на чувствителни одитни данни

10.1.6 P26 – Политика за сигурност на трети страни и доставчици: обхваща права на одит, документация за увереност и надзор върху съответствието на доставчици

10.1.7 P30 – Политика за реагиране при инциденти: съгласува одитите на процесите за обработване на инциденти с целите за увереност на СУИС

10.1.8 P32 – Политика за непрекъсваемост на дейността и аварийно възстановяване: изисква проверка на тестването за непрекъсваемост и съответствието с DRP по време на одитните цикли

11. Референтни стандарти и рамки

11.1 Тази политика е съгласувана с глобалните стандарти и правните изисквания за одит и непрекъснато валидиране на съответствието.

11.2 ISO/IEC 27001:

11.2.1 Клауза 9.2 – вътрешен одит: изисква редовни, базирани на риска одити на СУИС за оценка на ефективността и съответствието.

11.2.2 Клауза 9.3 – преглед от ръководството: резултатите от одита трябва да бъдат включвани в стратегическия преглед и подобрението.

11.2.3 Клауза 10.1 – несъответствие и коригиращо действие: одитните констатации трябва да бъдат адресирани чрез документирани CAPA процедури.

11.3 ISO/IEC 27002:2022 – Контроли 5.35–5.37:

11.3.1 Контроли от Приложение A 5.35–5.37: обхващат независим преглед, съответствие с правни/договорни изисквания и одитно регистриране.

11.3.2 Предоставят указания за внедряване за планиране, изпълнение и подобряване на програмите за одит и съответствие.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Оценки на контролите: изисква рутинен преглед на внедрените контроли за сигурност.

11.4.2 CA-5 – План за действия и ключови етапи (POA&M): съответства на проследяването и отстраняването на одитни констатации.

11.4.3 CA-7 – Непрекъснат мониторинг: подпомага проактивни, автоматизирани оценки на съответствието.

11.5 GDPR на ЕС (2016/679):

11.5.1 Членове 24 и 32: изискват доказателства за внедряването и ефективността на контролите за сигурност чрез подходящи структури на управление.

11.5.2 Член 33: подкрепя необходимостта от верифицирана одитна следа при реагиране при нарушения и уведомяване.

11.6 Директива NIS2 на ЕС (2022/2555):

11.6.1 Член 21(2)(g): изисква одитиране на политики и процедури като част от минималните мерки за управление на риска в киберсигурността.

11.6.2 Член 27: националните органи могат да извършват или да изискват одити за съществени и важни субекти.

11.7 DORA на ЕС (2022/2554):

11.7.1 Член 10(2)(e): субектите трябва да извършват вътрешни и външни одити на практиките за управление на ИКТ риска.

11.7.2 Член 25 – Изисквания за одит: налага периодични одити от вътрешни или независими външни одитори при регулаторна видимост.

11.8 COBIT 2019:

11.8.1 MEA01 – Мониторинг, оценяване и преценка на резултатността и съответствието: осигурява ефективността на контролите да бъде проверявана и докладвана на органите за управление.

11.8.2 MEA03 – Мониторинг, оценяване и преценка на съответствието: изисква съгласуване на организационните практики с правни, договорни и базирани на стандарти изисквания.