					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P08					Заглавие на документа: **Политика за осведоменост и обучение по информационна сигурност**							
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**

Съгласувано с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 7.3, Приложение A, Контрол 6.3	Определя изисквания за осведоменост и обучение, разгледани в настоящата политика
ISO/IEC 27002:2022	Контрол 6	Подкрепя подходящо обучение за осведоменост, съобразено с длъжностните роли
NIST SP 800-53 Rev.5	AT-1 до AT-5	Съответства на политиките и процедурите, обучението за осведоменост, ролево базираното обучение, записите от обучението и взаимодействието с групи по сигурността
EU GDPR	Членове 32, 39; Съображение 78	Изисква обучение за лицата, обработващи лични данни, и обща осведоменост на персонала
EU NIS2	Членове 21(2)(a, b), 21(3)	Изисква политики за обучение по риск и сигурност и инициативи за осведоменост
EU DORA	Членове 5, 8, 13	Изисква осведоменост и обучение относно ИКТ риска като част от контролите за устойчивост
COBIT 2019	APO07, DSS05, MEA	Подсилва осведомеността на работната сила, обучението на потребителите и непрекъснатия мониторинг на съответствието

1. Цел

1.1 Настоящата политика установява формалната рамка за гарантиране, че целият персонал е запознат със своите отговорности по информационна сигурност и получава необходимото обучение за защита на поверителността, целостта и наличността на информационните активи.

1.2 Политиката подпомага Клауза 7.3 от ISO/IEC 27001 и Приложение A, Контрол 6.3, като изисква структурирана програма за осведоменост и обучение, базирана на риска, съобразена с организационните роли и променящите се заплахи.

1.3 Политиката допринася за намаляване на уязвимостите, свързани с човешкия фактор, насърчаване на поведение, съобразено със сигурността, и непрекъснато утвърждаване на сигурни практики в съответствие с регулаторните и договорните изисквания.

2. Обхват

2.1 Настоящата политика се прилага за всички вътрешни и външни лица с достъп до организационни информационни системи, данни или съоръжения, включително:

2.1.1 Служители (на пълно работно време, непълно работно време, временни)

2.1.2 Външни изпълнители, консултанти, доставчици и стажанти

2.1.3 Трети страни с логически или физически достъп по силата на споразумения за услуги

2.2 Обхватът включва:

2.2.1 въвеждащо обучение за осведоменост по сигурността при постъпване

2.2.2 ролево специфично обучение (напр. разработчици, финанси, привилегировани потребители)

2.2.3 периодични опреснителни обучения и кампании за осведоменост

2.2.4 ad hoc обучение в отговор на инциденти или нови заплахи

2.3 Методите за предоставяне на обучение, обхванати от настоящата политика, включват електронно обучение, присъствени инструктажи, симулации, проверки на знанията, плакати, бюлетини по сигурността и задължителни потвърждения.

3. Цели

3.1 Да се гарантира, че целият персонал разбира своите отговорности за защита на организационните активи и за спазване на политиките за сигурност.

3.2 Да се осигури текущо и измеримо обучение за осведоменост, съгласувано с ролево базираната рискова експозиция.

3.3 Да се внедрят сигурни модели на поведение в ежедневните операции чрез утвърждаване на практики като сигурно използване на пароли, докладване на инциденти и устойчивост срещу фишинг.

3.4 Да се осигури регулаторно съответствие и готовност за одит по отношение на задължителните изисквания за обучение по информационна сигурност в различни индустрии и юрисдикции.

3.5 Да се намалят инцидентите по сигурността, произтичащи от небрежност, липса на осведоменост или неправилна преценка, чрез формиране на поведенчески модели и непрекъснато утвърждаване.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява стратегията на организацията за обучение по информационна сигурност и гарантира, че са осигурени необходимите ресурси и че тя е интегрирана в корпоративните приоритети.

4.1.2 Осъществява надзор на управленско ниво върху съответствието и осигурява спазването на политиката във всички отдели.

4.2 Директор по информационна сигурност (CISO) / Мениджър на СУИС

4.2.1 Отговаря за настоящата политика и определя рамката за осведоменост и обучение в съответствие с риска, съответствието и служебната необходимост.

4.2.2 Осъществява надзор върху проектирането, предоставянето, проследяването и прегледа на всички инициативи за обучение в областта на сигурността.

4.2.3 Гарантира, че обучението се актуализира периодично и отразява променящите се заплахи и нововъзникващите технологии.

[... 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 Честота на прегледа

9.1.1 Настоящата политика и свързаната с нея програма за обучение трябва да бъдат преглеждани:

9.1.1.1 Ежегодно, или

9.1.1.2 След значими инциденти, свързани с човешка грешка или вътрешна заплаха

9.1.1.3 При въвеждане на значими нови технологии или заплахи

9.1.1.4 В отговор на промени в правните, договорните или сертификационните задължения

9.2 Процес на преглед

9.2.1 Прегледът се ръководи от CISO в координация със:

9.2.1.1 ЧР и отделите по обучение

9.2.1.2 Длъжностните лица по правни въпроси и защита на данните

9.2.1.3 Функциите по ИТ сигурност и оперативен риск

9.2.2 Всички актуализации трябва да бъдат:

9.2.2.1 Одобрени от ръководния комитет на СУИС

9.2.2.2 Под управление на версиите и документирани в регистъра на документите на СУИС

9.2.2.3 Комуникирани към потребителите, ако съществените промени засягат обхвата на обучението или отговорностите

9.3 Управление на актуализациите на съдържанието

9.3.1 Обучителните модули и материалите за осведоменост трябва да бъдат преглеждани на всеки 12 месеца, за да се гарантира:

9.3.1.1 Актуалност спрямо средата на заплахите

9.3.1.2 Регулаторна точност

9.3.1.3 Съвместимост на формата (напр. достъпност, локализация)

9.3.2 Остаряло или подвеждащо съдържание трябва да бъде изтегляно незабавно и заменяно с одобрени алтернативи.

10. Свързани политики и връзки

10.1 Настоящата политика се подкрепя от следните политики и подпомага тяхното прилагане:

10.1.1 P01 – Политика за информационна сигурност: Установява осведомеността по сигурност като базова контролна мярка в СУИС на организацията.

10.1.2 P03 – Политика за допустима употреба: Изисква потвърждение от потребителя по време на обучението и изяснява отговорностите, свързани с ежедневното използване на технологии.

10.1.3 P07 – Политика за въвеждане в работата и прекратяване на правоотношенията: Гарантира, че обучението е вградено при постъпване и се проследява през целия период на заетост.

10.1.4 P06 – Политика за управление на риска: Свързва обучението, насочено към човешкия фактор, с моделирането на заплахи и стратегиите за намаляване на остатъчния риск.

10.1.5 P33 – Политика за одит и мониторинг на съответствието: Потвърждава, че контролите за осведоменост са действащи, измерими и ефективни по време на одити.

10.2 Заедно тези политики формират цялостна рамка за поведенчески контрол, която интегрира осведоменост, отчетност и културно утвърждаване.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 7.3 – Осведоменост: Изисква организациите да гарантират, че работещите са запознати с политиките за информационна сигурност и своите отговорности. Настоящата политика привежда това изискване в действие чрез структурирано въвеждане, периодично обучение и измеримо участие в кампании.

11.1.2 Приложение A, Контрол 6.3 – Осведоменост, образование и обучение по информационна сигурност: Напълно адресирано чрез първоначални, ролево базирани и текущи програми за обучение, съобразени с рисковите профили на потребителите.

11.2 ISO/IEC 27002:2022 – Контрол 6

11.2.1 Подкрепя разработването и предоставянето на обучение за осведоменост, подходящо за длъжностните роли, с акцент върху утвърждаването на сигурно поведение и периодичните актуализации въз основа на разузнаване за заплахи и обратна връзка от одити.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 до AT-5 (семейство „Осведоменост и обучение“): Настоящата политика съответства на AT-1 (Политика и процедури), AT-2 (Обучение за осведоменост), AT-3 (Ролево базирано обучение), AT-4 (Записи от обучения по сигурност) и AT-5 (Контакт с групи по сигурността).

11.3.2 IA-5, AC-2: Подсилва отговорността на потребителя за сигурна автентикация и допустима употреба — основни елементи от поведенческите резултати на програмите за осведоменост.

11.3.3 IR-1 до IR-8: Готовността за реагиране при инциденти се засилва чрез целенасочени кампании за осведоменост и симулации.

11.4 EU GDPR (2016/679)

11.4.1 Член 32 – Сигурност на обработването: Изисква персоналът, който обработва лични данни, да бъде обучен да разпознава, предотвратява и докладва рискове за личната информация. Настоящата политика гарантира, че лицата, обработващи данни, и всички относими роли са обучени по съответния начин.

11.4.2 Член 39 – Задачи на длъжностното лице по защита на данните: Включва повишаване на осведомеността и обучение на персонала, участващ в операции по обработване.

11.4.3 Съображение 78: Насърчава подходящи мерки за осведоменост с цел осигуряване на устойчиви практики за сигурност и спазване на политиките.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Член 21(2)(a, b): Изисква организациите да приемат политики за анализ на риска и обучение по сигурност за целия съответен персонал. Настоящата политика изпълнява това изискване чрез установяване на непрекъснати, съобразени с ролите процеси за обучение.

11.5.2 Член 21(3): Насърчава повишаването на осведомеността за риска в киберсигурността сред ръководството и персонала чрез инициативи за осведоменост и симулации.

11.6 EU DORA (2022/2554)

11.6.1 Член 13 – Стратегия за цифрова оперативна устойчивост: Изисква осведомеността и обучението относно ИКТ риска да бъдат част от модела на управление. Настоящата политика гарантира, че човешкият риск е адресиран чрез текущо обучение и симулации на заплахи.

11.6.2 Членове 5 и 8: Подчертават значението на рамките за вътрешен контрол, в които осведомеността и обучението са основни компоненти за ИКТ устойчивост и киберхигиена.

11.7 COBIT 2019

11.7.1 APO07 – Управление на човешките ресурси: Подсилва необходимостта от развитие на осведоменост относно отговорностите по сигурността и вграждането ѝ в управлението на работната сила.

11.7.2 DSS05 – Управление на услугите по сигурност: Установява контроли върху обучението на потребителите и докладването на инциденти, които са неразделна част от настоящата политика.

11.7.3 MEA03 – Мониторинг, оценяване и преценка на съответствието: Изисква преглед на ефективността на потребителското поведение и спазването на политиките — реализирано тук чрез фишинг тестове, тестове и показатели на кампаниите за осведоменост.