					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P08S					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	
ISO/IEC 27002:2022	Контрол 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU NIS2	Член 21(2)(i)	
EU DORA	Член 13	
COBIT 2019	BAI08, DSS	
EU GDPR	Член 32, 39	

1. Цел

1.1. Настоящата политика гарантира, че всички служители и външни изпълнители разбират своите отговорности по отношение на информационната сигурност.

1.2. Политиката има за цел да намали вероятността от човешка грешка, да подобри способността за откриване и докладване на инциденти и да насърчи култура на осведоменост по сигурността в цялата организация.

1.3. Политиката подпомага съответствието с ISO/IEC 27001, NIS2, GDPR и DORA, като утвърждава осведомеността по сигурността като част от ежедневното работно поведение и ролевите очаквания.

2. Обхват

2.1. Настоящата политика се прилага за всички служители, външни изпълнители, стажанти и трети страни, които имат достъп до системите или данните на дружеството.

2.2. Политиката обхваща:

2.2.1. въвеждащо обучение по осведоменост за информационна сигурност при постъпване на новоназначен персонал

2.2.2. ежегодно опреснително обучение по сигурност

2.2.3. ad hoc дейности за повишаване на осведомеността (напр. актуализации, свързани с инциденти, плакати или практически насоки)

2.3. Прилага се за всички длъжности, отдели и работни локации.

3. Цели

3.1. Да се гарантира, че целият персонал получава своевременно, разбираемо и относимо обучение по осведоменост за информационна сигурност.

3.2. Да се осигури на служителите способност да разпознават и избягват често срещани заплахи като фишинг, зловреден софтуер и изтичане на данни.

3.3. Да се осигури документиране на завършеното обучение с цел доказване на съответствие с правни, договорни и одитни изисквания.

3.4. Да се поддържа актуално съдържание на обучението, което отразява политиките, заплахите и приложимите регулаторни изисквания на организацията.

3.5. Да се насърчава проактивно мислене сред персонала, при което сигурността се възприема като част от ежедневните отговорности.

4. Роли и отговорности

4.1. Управител

4.1.1. Одобрява изискванията за обучение и гарантира осигуряването на необходимите ресурси.

4.1.2. Преглежда отчетите за завършено обучение и ескалира случаи на несъответствие, когато е необходимо.

4.2. Офис мениджър / Човешки ресурси (ЧР)

4.2.1. Координира провеждането на обучение за новоназначени служители и ежегодно опреснително обучение.

4.2.2. Поддържа записи и регистрационни дневници за обученията.

4.2.3. Осигурява потвърждение за запознаване от персонала с основните политики по информационна сигурност и споразумението за неразкриване на информация (NDA).

[... 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. Годишен преглед

9.1.1. Настоящата политика трябва да се преглежда ежегодно от управителя и ЧР, за да се гарантира, че отразява текущите рискове, регулации и потребности на персонала.

9.2. Междинни актуализации

9.2.1. Политиката и съдържанието на обучението трябва също да бъдат преглеждани и актуализирани след:

9.2.1.1. значим инцидент по сигурността

9.2.1.2. правни или договорни промени

9.2.1.3. организационно преструктуриране или миграция на системи

9.3. Управление на версиите и разпространение

9.3.1. Всяка актуализация трябва да включва:

9.3.1.1. номер на версията и дата на влизане в сила

9.3.1.2. обобщение на промените

9.3.1.3. одобрение от управителя

9.3.1.4. архив на всички предходни версии, съхраняван най-малко три години

9.4. Комуникация към служителите

9.4.1. Актуализациите на политиката трябва да се комуникират до целия персонал, а при съществени промени трябва да бъде получено потвърждение за запознаване.

10. Свързани политики и връзки

10.1. Настоящата политика подпомага следните документи:

10.1.1. P2S – Политика за роли и отговорности в управлението: определя отговорността за координация и надзор на обученията

10.1.2. P3S – Политика за допустима употреба: затвърждава очакванията за поведение, разглеждани в обучението

10.1.3. P4S – Политика за контрол на достъпа: гарантира, че потребителите разбират значението на сигурността на достъпа

10.1.4. P7S – Политика за въвеждане в работата и прекратяване на правоотношенията: интегрира обучението в процеса по постъпване

10.1.5. P30S – Политика за реагиране при инциденти: гарантира, че персоналът знае как да докладва инциденти своевременно и правилно

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 7.3 – Изисква организациите да гарантират, че персоналът е запознат със своите отговорности и въздействието върху сигурността

11.2. ISO/IEC 27002

11.2.1. Контрол 6.3 – Определя очакванията за обхвата и начина на провеждане на обучението по сигурност

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Изисква обучение за осведоменост за потребители с достъп до системи

11.3.2. AT-4 – Обхваща ролево базирано обучение и последиците при несъответствие

11.4. EU GDPR

11.4.1. Член 32 – Изисква мерки за сигурност, включително обучение на персонала, за защита на личните данни

11.4.2. Член 39 – Изисква длъжностните лица по защита на данните да упражняват надзор върху осведомеността и обучението, когато е приложимо

11.5. Директива EU NIS2

11.5.1. Член 21(2)(i) – Изисква текущи програми за осведоменост и обучение по киберсигурност

11.6. EU DORA

11.6.1. Член 13 – Изисква финансовите субекти да прилагат обучение и подготовка за целия персонал с отговорности, свързани с ИКТ

11.7. COBIT 2019

11.7.1. BAI08 – Управление на знанията: гарантира, че персоналът е компетентен и обучен

11.7.2. DSS05 – Управление на услугите по сигурност: подчертава осведомеността като ключов защитен контрол