					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P03S					Заглавие на документа: **Политика за допустима употреба**							
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 5	Относима към общия обхват на политиката и нейното прилагане
ISO/IEC 27002:2022	5.10, 5.11, 5	Насоки относно изискванията и контролите за допустима употреба
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Обхваща използването на системи и устройства, наблюдението и обучението на потребителите
GDPR на ЕС	Членове 5(1)(f), 32	Цялостност и поверителност на данните и мерки за сигурност
NIS2 на ЕС	Член 21(2)(b)	Изисква подходящи политики за сигурност и допустима употреба
DORA на ЕС	Член 9	Политика за управление на ИКТ риска, контроли и прилагане
COBIT 2019	DSS05, BAI	Услуги по сигурност и управление на знанията

1. Цел

1.1. Настоящата политика определя допустимата, отговорна и сигурна употреба на предоставените от дружеството системи, устройства, достъп до интернет, електронна поща, облачни услуги и всички лично притежавани устройства, използвани за служебни цели.

1.2. Тя гарантира, че лицата разбират своите задължения при използване на ИТ ресурсите на организацията, включително по отношение на защитата на целостта на данните, неприкосновеността на личния живот и непрекъсваемостта на дейността.

1.3. Настоящата политика подпомага съответствието с ISO/IEC 27001:2022 чрез въвеждане на ясни стандарти за поведение на потребителите, съобразени със законовите, договорните и регулаторните изисквания.

2. Обхват

2.1. Настоящата политика се прилага за всички лица, които осъществяват достъп до системите или данните на дружеството, администрират ги или работят с тях, включително:

2.1.1. Служители и изпълнители по договор

2.1.2. Временни служители и стажанти

2.1.3. Външни доставчици на ИТ услуги

2.2. Политиката обхваща:

2.2.1. Компютри, телефони и таблети, собственост на дружеството

2.2.2. Лично притежавани устройства, одобрени за служебна употреба (BYOD)

2.2.3. Мрежи на дружеството, облачни платформи и софтуерни услуги

2.2.4. Достъп до интернет, системи за електронна поща, споделени хранилища и бизнес приложения

2.3. Настоящата политика се прилага във всички работни среди — на място, дистанционно и в хибриден режим — и през цялото работно време.

3. Цели

3.1. Да се определи какво представлява допустима и недопустима употреба на ИТ системите.

3.1.1. Да се намалят рисковете за сигурността, произтичащи от неправомерна употреба, неразрешен достъп или въвеждане на зловреден софтуер.

3.1.2. Да се защитят бизнес данните, информацията за клиентите и репутацията на дружеството.

3.1.3. Да се установят правила, подлежащи на прилагане, и да се осигури отчетност за всички потребители.

3.1.4. Да се подпомогнат наблюдението и съответствието с цел ранно откриване на нарушения и предприемане на коригиращи действия.

4. Роли и отговорности

4.1. Управител

4.1.1. Одобрява настоящата политика и носи отговорност за осигуряване на необходимите ресурси и правомощия за нейното прилагане.

4.1.2. Преглежда и одобрява всички изключения от настоящата политика.

4.2. ИТ мениджър или външен доставчик на ИТ услуги

4.2.1. Поддържа инвентаризационен списък на одобрения софтуер и хардуер.

4.2.2. Конфигурира устройствата така, че да се прилагат правилата за допустима употреба (напр. филтриране на съдържание, регистриране на достъпа).

4.2.3. Наблюдава употребата за потенциални нарушения и разследва инциденти.

4.2.4. Осигурява лично притежаваните устройства (BYOD), използвани за служебни цели, да са разрешени и защитени.

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

9. Изисквания за преглед и актуализиране

9.1. Годишен преглед

9.1.1. Настоящата политика се преглежда ежегодно от ИТ мениджъра, с окончателно одобрение от управителя, за да се гарантира, че остава съобразена с моделите на използване на технологиите, възникващите рискове и задълженията за съответствие.

9.2. Основания за извънреден преглед

9.2.1. Прегледи се извършват и в отговор на:

9.2.2. Нови системи или технологии (напр. нова облачна услуга или платформа за крайни устройства)

9.2.3. Съществени нарушения на политиката

9.2.4. Актуализирани закони или договорни условия, засягащи използването на ИТ

9.3. Документиране на промените

9.3.1. Всички актуализации трябва да се записват в регистър на версиите, който включва:

9.3.1.1. Номер на версия

9.3.1.2. Дата на преглед

9.3.1.3. Обобщение на промените

9.3.1.4. Одобряващ орган

9.4. Комуникиране на политиката

9.4.1. Актуализираните версии на настоящата политика трябва да бъдат предоставяни на всички засегнати потребители. Служителите трябва да потвърдят получаването и разбирането ѝ като част от своите задължения по информираност за сигурността.

10. Свързани политики и зависимости

10.1. Настоящата политика се прилага съвместно с няколко други политики за МСП, за да се осигури цялостно покритие на отговорностите по сигурността:

10.1.1. P4S – Политика за контрол на достъпа: Определя техническото и процедурното прилагане на разрешената употреба и ограниченията върху акаунтите.

10.1.2. P8S – Политика за информираност и обучение по информационна сигурност: Осигурява обучение на потребителите относно границите на допустимата употреба и задълженията за докладване.

10.1.3. P9S – Политика за дистанционна работа: Регламентира използването на системите на дружеството извън офиса или в домашна среда.

10.1.4. P17S – Политика за защита на данните и поверителност: Установява правила за обработване на лични данни, които се пресичат с наблюдението на допустимата употреба и BYOD.

10.1.5. P30S – Политика за реагиране при инциденти: Урежда процедурите за разследване и реакция при неправомерна употреба или нарушения на правилата за допустима употреба.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 5.10 – Изисква организациите да определят и прилагат правила за допустима употреба на информационните активи.

11.2. ISO/IEC 27002

11.2.1. Контрол 5.10 – Предоставя насоки за допустима употреба на системите, включително разрешено и забранено поведение.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Разглежда контрола върху използването на системите, включително лично притежавани устройства.

11.3.2. AC-20 – Изисква разрешаване и наблюдение на външни системи.

11.3.3. AT-2 – Подчертава обучението на потребителите относно практиките за допустима употреба.

11.4. GDPR на ЕС

11.4.1. Член 5(1)(f) – Изисква целостта и поверителността на личните данни, които могат да бъдат компрометирани при неправомерна употреба от потребители.

11.4.2. Член 32 – Изисква прилагането на технически и организационни мерки за защита на системите и данните.

11.5. NIS2 на ЕС

11.5.1. Член 21(2)(b) – Изисква подходящи политики за сигурност, включително правила за допустима употреба, за ограничаване на киберзаплахите.

11.6. DORA на ЕС

11.6.1. Член 9 – Изисква политики за управление на ИКТ риска, които включват контроли върху използването и механизми за прилагане.

11.7. COBIT 2019

11.7.1. DSS05 – Управление на услугите по сигурност: Подчертава основан на политики контрол върху поведението на потребителите.

11.7.2. BAI08 – Управление на знанията: Разглежда информираността относно отговорностите по политиките и обучението за допустима употреба.