					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P03					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**

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 5	Установява норми на поведение и изисквания за Политиката за допустимо използване (AUP)
ISO/IEC 27002:2022	Контроли 6.1, 6.2, 8.1, 8	Предоставя насоки относно отговорностите по информационна сигурност, осведомеността и управлението на устройства и данни
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Контроли за достъп и за осведоменост/поведение, приложими към използването на ИТ активи
GDPR на ЕС	Членове 5(1)(f), 32; Съображение 39	Налага изисквания за поверителност и цялостност, изисква технически и организационни мерки и правно основание за правилното използване
NIS2 на ЕС	Член 21(2)(a–d)	Изисква оперативни политики и обучение за сигурно използване
DORA на ЕС	Член 5	Подпомага управлението на ИКТ риска чрез регламентиране на поведението на потребителите
COBIT 2019	APO07, BAI05, DSS05, MEA01	Човешки ресурси, управление на промените, управлявана сигурност, наблюдение на съответствието и резултатността

1. Цел

1.1 Настоящата политика определя допустимото и недопустимото използване на информационните системи на организацията, изчислителните ресурси, комуникационните средства и практиките за обработване на данни.

1.2 Тя гарантира, че всички потребители разбират своите отговорности при използването на корпоративните ИТ активи и че действията им подпомагат поверителността, цялостността и наличността (CIA), както и законосъобразното обработване на информацията.

1.3 Политиката изпълнява изискванията на ISO/IEC 27001:2022, клауза 5.10, като установява норми на поведение при използването на системи и въвежда технически и процедурни защитни мерки за свеждане до минимум на риска от неправомерно използване, небрежност или злоупотреба.

1.4 Тя също така подпомага дейностите по разследване и прилагане на политиката, включително реагиране при инциденти и налагане на дисциплинарни мерки при нарушения.

2. Обхват

2.1 Настоящата политика се прилага за всички физически и юридически лица, на които е предоставен достъп до информационните системи и активите на организацията, включително, но не само:

2.1.1 Служители, външни изпълнители, консултанти, стажанти и персонал, предоставен от агенции

2.1.2 Доставчици от трети страни със системен достъп или с делегирани административни роли

2.1.3 Гости или партньори, използващи притежавана от организацията или разрешена ИТ инфраструктура

2.2 Обхватът включва всички технологични и информационни активи на организацията, включително:

2.2.1 Работни станции, преносими компютри, мобилни устройства и сървъри

2.2.2 Мрежова инфраструктура и облачно хоствани услуги

2.2.3 Електронна поща, средства за съобщения, съхранение на файлове, платформи за сътрудничество и VPN

2.2.4 Данни в покой, при пренос или в процес на обработване, независимо от формата или местоположението им

2.2.5 Всяко лично устройство, използвано в рамките на политиката за използване на лични устройства (BYOD), което се свързва към системите на организацията

2.3 Настоящата политика се прилага във всички работни среди, включително:

2.3.1 Корпоративни офиси и производствени обекти

2.3.2 Локации за дистанционна работа или хибридни режими на работа

2.3.3 Операции на терен или обекти, управлявани от трети страни

2.4 Всички потребители са длъжни да потвърдят запознаването си с тази политика и да я спазват като условие за достъп до фирмени системи или за обработване на корпоративни данни.

3. Цели

3.1 Да определя и налага правила за разрешено използване на ИТ ресурсите.

3.2 Да предотвратява неоторизиран достъп, изтичане на данни или щети в резултат на небрежно или злонамерено използване.

3.3 Да защитава мрежите, активите и данните на дружеството от заплахи, породени от поведението на потребителите.

3.4 Да подпомага изпълнението на правните и договорните задължения чрез демонстриране на надлежна грижа при управлението на ИТ ресурсите.

3.5 Да осигурява последователност и яснота при прилагането на дисциплинарни мерки и процесите за управление на изключения.

3.6 Да насърчава култура на етично, сигурно и отговорно използване на цифрови и физически изчислителни ресурси.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява Политиката за допустимо използване (AUP) и гарантира, че тя е съгласувана с бизнес целите, регулаторните изисквания и ценностите на организацията.

4.1.2 Осигурява ресурси за прилагане на политиката, обучение, мониторинг и преглед на политиката.

4.1.3 Преглежда състоянието на съответствието и дисциплинарните мерки, свързани с нарушения на политиката, като част от управлението на СУИС.

4.2 Екипи по ИТ и информационна сигурност

4.2.1 Прилагат технически защитни мерки за изпълнение на настоящата политика, включително:

4.2.2 Филтриране на съдържание, средства за защита от зловреден софтуер, защита на крайни точки и инструменти за мрежов мониторинг

4.2.3 Конфигурации за сигурност на електронната поща и решения за предотвратяване на загуба на данни (DLP)

4.2.4 Черни списъци и списъци с разрешени елементи за софтуер, хардуер и уебсайтове

4.2.5 Поддържат регистър на одобрените и забранените софтуери, устройства и услуги.

4.2.6 Разследват предполагаеми нарушения на AUP, събират цифрови доказателства и при необходимост подпомагат дисциплинарни или правни действия.

4.2.7 Сътрудничат с отдел „Човешки ресурси“ и правния отдел по процедурите за обработване на инциденти, ескалация и задълженията за докладване.

[... 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 Основания и периодичност за преглед

9.1.1 Настоящата политика трябва да бъде преглеждана:

9.1.1.1 Най-малко веднъж годишно

9.1.1.2 След всяка съществена промяна в технологиите или инфраструктурата

9.1.1.3 След инциденти или одитни констатации, които показват пропуски в прилагането на политиката

9.1.1.4 В отговор на промени в приложимото законодателство или договорни изисквания

9.2 Собственост и одобрение

9.2.1 Директорът по информационна сигурност или определеният мениджър на СУИС отговаря за процеса по преглед.

9.2.2 Актуализациите трябва да бъдат одобрявани от изпълнителното ръководство и комуникирани в цялата организация.

9.2.3 Потвърждението на актуализираните условия трябва да бъде събрано отново при повторно издаване на политиката.

9.3 Управление на документа

9.3.1 Политиката трябва да включва следните метаданни и данни за версиите:

9.3.1.1 Заглавие, идентификатор и ниво на класификация

9.3.1.2 Собственик на политиката и отговорник за документа

9.3.1.3 История на промените и обосновка за актуализациите

9.3.1.4 Дати на преглед и следваща планирана актуализация

9.3.1.5 Препратки към журналите за разпространение и потвърждение

9.3.2 Контролираното оригинално копие трябва да се съхранява в хранилището за документи на СУИС под управление на версиите.

10. Свързани политики и зависимости

10.1 Настоящата политика трябва да се тълкува съвместно със следните документи:

10.1.1 P1 – Политика за информационна сигурност: Установява базовите очаквания за поведение и ангажираността на висшето ръководство към допустимото използване.

10.1.2 P4 – Политика за контрол на достъпа: Определя разрешенията и правата, свързани с потребителите, системите и достъпа до данни, като пряко прилага границите на допустимото използване.

10.1.3 P6 – Политика по управление на риска: Разглежда рисковете, свързани с поведението, и подпомага дейностите по мониторинг и третиране, свързани със заплахи, породени от действията на потребителите.

10.1.4 P7 – Политика за въвеждане в работата и прекратяване на правоотношенията: Гарантира, че условията за допустимо използване се потвърждават при постъпване и се отнемат при напускане.

10.1.5 P9 – Политика за дистанционна работа: Разширява правилата за допустимо използване към дистанционни и хибридни работни среди.

10.2 Тези свързани политики формират многослоен модел на защита за поведенско, техническо и договорно управление.

11. Референтни стандарти и рамки

11.1 Настоящата Политика за допустимо използване (AUP) е съгласувана с международно признати стандарти и правни рамки, за да осигури приложими, подлежащи на одит и базирани на риска контроли върху поведението при всяко използване на цифрови и физически информационни системи.

11.2 ISO/IEC 27001:2022

11.2.1 Клауза 5.10 – Допустимо използване на информация и други свързани активи: Настоящата политика пряко изпълнява изискването да се определят, комуникират и прилагат правила за подходящо използване на ИТ ресурсите.

11.2.2 Приложение A, Контрол 6.1 – Отговорност за информационната сигурност: Възлага ясни отговорности за поведението на потребителите и надзора по съответствие.

11.2.3 Приложение A, Контрол 6.2 – Осведоменост, образование и обучение по информационна сигурност: Вградените процеси за обучение и потвърждение за запознаване с политиката са част от прилагането на AUP.

11.2.4 Приложение A, Контрол 8.1 – Потребителски крайни устройства и 8.12 – Предотвратяване на загуба на данни: Разглежда допустимото поведение при използване на потребителски устройства и урежда дейности, които могат да доведат до разкриване или изтичане на данни.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Контрол на достъпа за мобилни устройства) и AC-20 (Използване на външни информационни системи): Настоящата политика определя задълженията и ограниченията за потребителите при BYOD и достъп до системи на трети страни.

11.3.2 PL-4 (Правила за поведение): Предоставя подробни изисквания за допустимо използване, съответстващи на тази политика.

11.3.3 AT-2 (Обучение за осведоменост по сигурността): Подпомага се чрез обучение на потребителите и документирано потвърждение за запознаване с политиката.

11.3.4 AU-2 (Одитни събития) и AU-12 (Генериране на одит): Прилагането се основава на мониторинг на действията на потребителите и предупреждения при нарушения.

11.4 GDPR на ЕС (2016/679):

11.4.1 Член 5(1)(f): Налага изисквания за сигурност и цялостност на личните данни; тази политика смекчава рисковете, породени от човешко поведение и неоторизирано използване.

11.4.2 Член 32: Изисква технически и организационни мерки — като контроли върху поведението и ограничения на използването — за защита на личните данни.

11.4.3 Съображение 39: Подчертава необходимостта да се гарантира само необходимият достъп и законосъобразното използване на данните от оправомощени лица.

11.5 Директива NIS2 на ЕС (2022/2555):

11.5.1 Член 21(2)(a–d): Изисква оперативни политики и обучение за сигурно използване на системите, което настоящата AUP осигурява чрез определяне на поведение, мониторинг и процеси по прилагане.

11.6 DORA на ЕС (2022/2554):

11.6.1 Член 5: Настоящата политика подпомага рамката за управление на ИКТ риска чрез определяне на правила за взаимодействието човек–система и свеждане до минимум на рисковата експозиция от киберрискове, породени от поведение.

11.7 COBIT 2019:

11.7.1 APO07 – Управлявани човешки ресурси: Прилага отговорностите и осведомеността на потребителите в рамките на целия жизнен цикъл на служителя.

11.7.2 BAI05 – Управлявана организационна промяна: Вгражда управлението на допустимото използване в процесите на промяна, които влияят върху поведението на потребителите.

11.7.3 DSS05 – Управлявани услуги по сигурност: Подпомага мониторинга на потребителската активност, поведенческите предупреждения и механизмите за автоматизиран отговор.

11.7.4 MEA01 – Мониторинг, оценяване и преценка на резултатността и съответствието: Политиката определя показатели и механизми за валидиране на съответствието на потребителите с очакваното поведение.