					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P09S					Заглавие на документа: **Политика за дистанционна работа**							
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 6.1, 6.2, 8	
ISO/IEC 27002:2022	Контрол 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Директива NIS2 на ЕС	Членове 21(2)(b), 21(2)(h)	NIS2
Регламент DORA на ЕС	Член 9	DORA
COBIT 2019	DSS05, APO13	COBIT 2019
ОРЗД на ЕС	Член 32	ОРЗД

1. Цел

1.1 Настоящата политика определя изискванията за сигурност за служители и външни изпълнители, които работят дистанционно, включително от дома, от споделени работни пространства или по време на пътуване.

1.2 Тя има за цел да защити поверителността, целостта и наличността на служебната информация, до която се осъществява достъп извън средите, контролирани от дружеството.

1.3 Настоящата политика осигурява съответствие с международните стандарти и намалява рискове като неоторизиран достъп, загуба на данни и прекъсване на услугите.

2. Обхват

2.1 Настоящата политика се прилага за всички членове на персонала (служители, външни изпълнители, консултанти и временни работници), които осъществяват достъп до системи, мрежи или данни на дружеството при работа извън обектите на организацията.

2.2 Тя обхваща:

2.2.1 използването на предоставени от дружеството и лично притежавани устройства

2.2.2 достъп чрез VPN, отдалечен работен плот или облачни услуги

2.2.3 сигурно боравене с информация извън помещенията на дружеството

2.2.4 мониторинг, обработване на изключения и прилагане на политиката

2.3 Политиката се прилага както за постоянни, така и за частични режими на дистанционна работа, включително ad hoc отдалечен достъп.

3. Цели

3.1 Да се предотврати неоторизиран достъп до системите на дружеството или чувствителни данни по време на дистанционна работа.

3.2 Да се гарантира, че устройствата и комуникационните връзки, използвани извън офиса, отговарят на изискванията за базова сигурност.

3.3 Да се поддържа контрол върху привилегиите за отдалечен достъп и мониторинга.

3.4 Да се предоставят ясни указания на служителите и ръководителите за сигурни практики при дистанционна работа.

3.5 Да се осигури съответствие с изискванията на ISO, NIS2, ОРЗД, DORA и COBIT по отношение на дистанционната и мобилната работа.

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява режимите на дистанционна работа и следи за съответствието.

4.1.2 Ескалира инциденти по сигурността или повтарящи се несъответствия.

4.1.3 Преглежда изключенията и осигурява последващи действия по инциденти.

4.2 ИТ поддръжка или външен доставчик на ИТ услуги

4.2.1 Осигурява защитен отдалечен достъп (напр. VPN, MFA).

4.2.2 Прилага мерки за сигурност на крайните точки, криптиране и конфигурации на устройствата.

4.2.3 Подпомага потребителите и разследва технически проблеми, свързани със сигурността.

[... 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 на политиката

9.1.1 Управителят и ИТ поддръжката трябва да преглеждат настоящата политика ежегодно, за да я съгласуват с промените в технологиите, работната сила и правната рамка.

9.2 Основания за по-ранна актуализация

9.2.1 Незабавен преглед се изисква след:

9.2.1.1 съществен инцидент по сигурността, свързан с дистанционна работа

9.2.1.2 промени в изискванията на NIS2, ОРЗД или DORA

9.2.1.3 преминаване към нова технология за отдалечен достъп (напр. различна VPN платформа)

9.3 Управление на версиите и архивиране

9.3.1 Всички версии на настоящата политика трябва да бъдат:

9.3.1.1 датирани и одобрени от Управителя

9.3.1.2 с обозначен номер на версия

9.3.1.3 архивирани за срок от най-малко три години

9.4 Комуникация към персонала

9.4.1 Актуализациите на политиката трябва да бъдат съобщавани на всички дистанционни потребители. За всяка съществена промяна се изисква потвърждение за запознаване с политиката.

10. Свързани политики и обвързаности

10.1 Настоящата политика е свързана със следните документи и ги подпомага:

10.1.1 P2S – Политика за роли и отговорности в управлението: Определя кой разрешава и упражнява надзор върху отдалечения достъп

10.1.2 P4S – Политика за контрол на достъпа: Определя изискванията за сигурно предоставяне и отнемане на отдалечен достъп

10.1.3 P6S – Политика за управление на риска: Проследява и оценява рисковете, свързани с достъп извън обектите на организацията

10.1.4 P8S – Политика за осведоменост и обучение по информационна сигурност: Обучава потребителите относно рисковете при дистанционна работа и добрите практики

10.1.5 P30S – Политика за реагиране при инциденти: Управлява реакцията при инциденти, свързани с отдалечен достъп, като изтичане на идентификационни данни или загуба на устройство

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.1 – Планиране, основано на риска, за сценарии на отдалечен достъп

11.1.2 Клауза 6.2 – Разглежда отговорностите на Човешки ресурси (ЧР) в контекст на мобилна и дистанционна работа

11.1.3 Клауза 8.1 – Оперативно планиране и контрол на отдалечени процеси

11.2 ISO/IEC 27002

11.2.1 Контрол 6.7 – Предоставя практически насоки за сигурност при дистанционна и мобилна работа

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Контрол на отдалечения достъп, защита на сесиите и наблюдение на сигурността

11.3.2 AC-2 – Контрол на потребителски акаунти за лица извън обектите на организацията

11.4 ОРЗД на ЕС

11.4.1 Член 32 – Изисква защита на данните „още при проектирането и по подразбиране“, включително в дистанционна среда

11.5 Директива NIS2 на ЕС

11.5.1 Член 21(2)(b) – Изисква сигурно използване на мрежови и информационни системи

11.5.2 Член 21(2)(h) – Изисква мерки за сигурност, свързани с ЧР, включително контроли извън обектите на организацията

11.6 Регламент DORA на ЕС

11.6.1 Член 9 – Изисква финансовите субекти да поддържат устойчивост на ИКТ във всички режими на работа, включително при отдалечен достъп

11.7 COBIT 2019

11.7.1 DSS05 – Мониторинг, оценяване и преценка на услугите по сигурността: включва защита на крайните точки и сигурни практики за дистанционна работа

11.7.2 APO13 – Управлявана сигурност: осигурява сигурно предоставяне и надзор на риска при мобилен и отдалечен достъп