<table>
<tr><td colspan="5"></td><td colspan="7">Въведете тук наименованието на регистрираното юридическо лице</td></tr>
<tr><td colspan="5">Номер на документа:
P09</td><td colspan="7">Заглавие на документа:
Политика за дистанционна работа</td></tr>
<tr><td colspan="2">Версия:
1.0</td><td colspan="3">Дата на влизане в сила:
01.01.2025</td><td colspan="7">Собственик на документа:</td></tr>
<tr><td>X</td><td>Политика</td><td></td><td>Стандарт</td><td></td><td>Процедура</td><td></td><td>Формуляр</td><td></td><td>Регистър</td><td></td><td>Друго</td></tr>
</table>

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

1. Цел

1.1 Настоящата политика определя задължителните изисквания за сигурно осъществяване на дистанционна работа, включително използването на организационни системи, достъпа до данни и изпълнението на служебни задължения извън корпоративните помещения.

1.2 Тя осигурява поверителността, целостта и наличността на информационните активи, до които се осъществява отдалечен достъп, и установява контроли за смекчаване на рисковете, свързани с разпределени работни среди.

1.3 Политиката изпълнява изискванията на ISO/IEC 27001:2022, Приложение A, Контрол 6.7, чрез прилагане на технически и процедурни мерки, съобразени с условията на дистанционна работа.

2. Обхват

2.1 Настоящата политика се прилага за целия персонал, на който е разрешено да работи дистанционно, включително:

2.1.1 Служители (на пълно работно време, непълно работно време и по договор)

2.1.2 Външни доставчици на услуги, консултанти и други трети страни

2.1.3 Временни служители и персонал по проекти с одобрен отдалечен достъп

2.2 Политиката обхваща:

2.2.1 Достъп до организационни системи чрез VPN или одобрени инструменти за отдалечен достъп

2.2.2 Обработване на чувствителна и регулирана информация извън защитени обекти

2.2.3 Използване на оборудване, собственост на организацията, или на лични устройства (BYOD)

2.2.4 Физически и логически мерки за защита в отдалечени среди

2.3 Политиката се прилага за всички географски местоположения и часови зони, в които организацията разрешава дистанционна работа, независимо дали е регулярна, ad hoc или по време на събития, свързани с непрекъсваемостта на дейността.

3. Цели

3.1 Да се гарантира, че само упълномощени лица могат да осъществяват отдалечен достъп до вътрешни системи и информация.

3.2 Да се осигури прилагането на криптиране, многофакторно удостоверяване (MFA) и защита на крайните точки по всички канали за отдалечен достъп.

3.3 Да се поддържа устойчива позиция по сигурността спрямо заплахи като фишинг, зловреден софтуер, неоторизирано извличане на данни и неразрешено излагане на системи.

3.4 Да се регламентира как чувствителните данни се предават, съхраняват или разпечатват в среди извън обектите на организацията.

3.5 Да се въведат мерки за физическа сигурност, които ограничават видимостта и неоторизираното наблюдение по време на отдалечени сесии.

3.6 Да се спазват международните регулаторни изисквания, свързани с отдалечения достъп до данни, включително GDPR, NIS2 и DORA.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява тази политика и осигурява необходимите ресурси и интегрирането ѝ в дейностите на Човешки ресурси (ЧР), ИТ и информационната сигурност.

4.1.2 Утвърждава критериите за допустимост за дистанционна работа в организацията и приложимостта им по бизнес звена.

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

4.2.1 Отговаря за политиката, поддържа я и гарантира съответствието ѝ с рисковия профил и регулаторните изисквания.

4.2.2 Определя контролите за сигурност при отдалечен достъп (напр. криптиране, защита на крайните точки, таймаути на сесиите).

4.2.3 Одобрява обработването на изключения и наблюдава ефективността на контролите.

[... 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 преглед

9.1.1 Настоящата политика трябва да се преглежда ежегодно или по-често при:

9.1.1.1 Въвеждане на нови технологии за отдалечен достъп

9.1.1.2 Значително разширяване на дистанционната работа (напр. инициативи за хибридна работна сила)

9.1.1.3 Поява на нови заплахи, уязвимости или инциденти, свързани с отдалечени среди

9.1.1.4 Промени в приложимите правни или регулаторни рамки

9.2 Собственост и процес на преглед

9.2.1 Собственик на политиката е Директорът по информационна сигурност (CISO). Прегледът трябва да се координира с:

9.2.1.1 ИТ операции и архитектура

9.2.1.2 Човешки ресурси (ЧР) и Управление на съоръжения и активи (за оперативните последици и отражението върху работните пространства)

9.2.1.3 Длъжностното лице по защита на данните (за контролите за поверителност и трансграничните данни)

9.2.2 Актуализациите на политиката трябва да бъдат:

9.2.2.1 Одобрени от Ръководния комитет по СУИС

9.2.2.2 Комуникирани до всички засегнати служители и външни изпълнители

9.2.2.3 Интегрирани в материалите за въвеждане и ежегодното опреснително обучение

9.3 Контрол на документа и разпространение

9.3.1 Политиката трябва да включва управление на версиите, дата на влизане в сила и история на промените.

9.3.2 Заменените версии трябва да се съхраняват съгласно Политиката за управление на документи (P14).

9.3.3 Ревизираните версии трябва да задействат задължително повторно потвърждение за запознаване от потребителите, допустими за дистанционна работа.

10. Свързани политики и връзки

10.1 Настоящата политика се прилага съвместно със:

10.1.1 P1 – Политика за информационна сигурност: Установява базовите изисквания за сигурно боравене с активи, приложими за всички работни среди, включително отдалечените.

10.1.2 P3 – Политика за допустима употреба: Регламентира подходящото използване на организационни устройства и системи по време на сесии за дистанционна работа.

10.1.3 P4 – Политика за контрол на достъпа: Гарантира, че привилегиите за отдалечен достъп следват принципа на минималните привилегии и подходящите механизми за удостоверяване.

10.1.4 P6 – Политика за управление на риска: Определя как рисковете при дистанционна работа се идентифицират, третират и наблюдават в рамките на СУИС.

10.1.5 P12 – Политика за управление на активите: Изисква инвентаризация и управление на конфигурацията за всички устройства, използвани отдалечено.

10.1.6 P22 – Политика за регистриране и мониторинг: Гарантира, че отдалечените сесии се наблюдават, подлежат на одит и се съхраняват съгласно изискванията за съответствие.

10.1.7 P14 – Политика за съхранение и унищожаване на данни: Определя правилата за обработване на данни, приложими към дистанционната работа, включително сменяеми носители и унищожаване на устройства.

10.2 Тези политики съвместно гарантират, че дистанционната работа е сигурна, съответства на изискванията и е приложима във всички функции и географски местоположения.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати рамки за сигурност, защита на данните и управление на ИКТ риска, за да осигури сигурни, проследими и съответстващи на изискванията практики за дистанционна работа.

11.2 ISO/IEC 27001

11.2.1 Клауза 6.1.3 – Планиране на третирането на риска: Настоящата политика допринася за третирането на рисковете, свързани с отдалечения достъп и разпределените работни среди.

11.2.2 Клауза 8.1 – Оперативно планиране и контрол: Изисква прилагането на контроли за системи, до които се осъществява достъп извън помещенията на организацията.

11.2.3 Приложение А, Контрол 6.7 – Дистанционна работа: Настоящата политика изцяло адресира изискваните контроли за информационна сигурност, когато персоналът работи извън помещенията на организацията, включително физически и логически мерки за защита, управление на правата за достъп и мониторинг на поведението на потребителите.

11.3 ISO/IEC 27002:2022 – Контрол 6

11.3.1 Този контрол изисква процедурни и технически мерки за дистанционна работа. Той включва изисквания за сигурност на устройствата, методи за достъп, обработване на данни, мерки за защита на средата и управление на трети страни — всички от които се прилагат чрез настоящата политика.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Отдалечен достъп): Поддържа се пряко чрез VPN контроли, MFA, журналиране на сесиите и упълномощаване за достъп, базирано на роли, за отдалечени потребители.

11.4.2 AC-2 (Управление на акаунти): Контролира допустимостта за достъп, предоставянето на отдалечени привилегии и деактивирането на акаунти.

11.4.3 SC-12 до SC-13 (Криптографска защита, установяване на криптографски ключове): Прилагат се чрез задължително използване на VPN и пълнодисково криптиране за отдалечени крайни точки.

11.4.4 MP-5 (Защита при транспортиране на носители) и PE-18 (Местоположение на компонентите на информационната система): Указанията за дистанционна работа изискват защита при пренос и физически мерки за защита в среди извън обектите на организацията.

11.4.5 AU-2, AU-6: Журналирането и мониторингът на отдалечени сесии подпомагат изискванията за одит и реагиране при инциденти.

11.5 GDPR на ЕС (2016/679)

11.5.1 Член 32 – Сигурност на обработването: Настоящата политика налага контроли за сигурност на отдалечения достъп, криптиране и журналиране, необходими за защита на личните данни, до които се осъществява достъп или които се обработват отдалечено.

11.5.2 Член 5(1)(f): Гарантира, че личните данни, до които се осъществява достъп извън обекта, са защитени срещу неоторизирано или незаконосъобразно обработване и случайна загуба.

11.5.3 Съображение 39: Подчертава ограничаването на достъпа, целостта и поверителността — особено когато устройствата напускат защитени помещения.

11.6 Директива NIS2 на ЕС (2022/2555)

11.6.1 Член 21(2)(a, b, d): Изисква отдалеченият достъп да бъде защитен като част от рамката за управление на ИКТ риска на организацията. Настоящата политика изпълнява изискването за мерки за сигурност, които обхващат контрол на достъпа, сигурност на данните и организационни политики за отдалечени среди.

11.6.2 Член 21(3): Насърчава осведомеността по сигурността и прилагането на политиките сред персонала, работещ извън централните помещения.

11.7 DORA на ЕС (2022/2554)

11.7.1 Член 5 – Рамка за управление и вътрешен контрол: Настоящата политика подпомага очакванията за контрол на ИКТ риска за всички оперативни сценарии, включително хибридни и отдалечени модели.

11.7.2 Член 8 – Рамка за управление на ИКТ риска: Рисковете при отдалечен достъп се идентифицират, смекчават и управляват чрез технически и организационни контроли, прилагани с настоящата политика.

11.7.3 Член 9 – Механизми за споделяне на информация: Защитава срещу отдалечено изтичане на информация, споделяна в мрежи за цифрова оперативна устойчивост.

11.8 COBIT 2019

11.8.1 DSS01 – Управлявани операции: Настоящата политика подпомага сигурната непрекъсваемост на бизнес операциите независимо от физическото местоположение.

11.8.2 BAI06 – Управлявани ИТ промени и BAI09 – Управлявани активи: Гарантират, че устройствата за дистанционна работа се проследяват, конфигурират сигурно и се третират като критични активи.

11.8.3 APO13 – Управлявана сигурност: Насърчава определена рамка за управление на сигурността за отдалечени среди.

11.8.4 MEA03 – Мониторинг, оценяване и преценка на съответствието: Установява, че дейностите по дистанционна работа трябва да бъдат регистрирани, преглеждани и одитирани.