					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P21S					Заглавие на документа: **Политика за мрежова 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**

Правна бележка (авторски права и ограничения за ползване)

(C) 2025 Clarysec LLC. All rights reserved.

Настоящият документ е интелектуална собственост на Clarysec LLC. Никоя част от него не може да бъде копирана, използвана повторно, разпространявана или изменяна за търговски или внедрителски цели без изрично писмено разрешение.

Неупълномощеното използване е строго забранено и може да доведе до правни действия.

За лицензиране се свържете с: info@clarysec.com

Съгласуване със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	-
ISO/IEC 27002:2022	Контрол 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR на ЕС	Член 32	-
NIS2 на ЕС	Членове 21(2)(d), (e)	-
DORA на ЕС	Членове 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Цел

1.1. Целта на настоящата политика е да гарантира, че всички вътрешни и външни мрежови комуникации са защитени срещу неразрешен достъп, подправяне, подслушване или злоупотреба чрез ясно определени контроли за сигурност.

1.2. Политиката определя правила за сигурно проектиране, използване и управление на мрежовата инфраструктура, включително маршрутизатори, безжични точки за достъп, връзки за отдалечен достъп и сегментирани мрежи.

1.3. Тя има за цел да сведе до минимум експозицията към интернет базирани заплахи, да осигури поверителността на данните, предавани по вътрешни и външни мрежи, и да поддържа наличността на критичните услуги.

1.4. Настоящата политика подпомага сертифицирането по ISO/IEC 27001:2022 и допринася пряко за изпълнението на правни и регулаторни задължения по GDPR, NIS2 и DORA, като същевременно осигурява техническа обоснованост пред клиенти и одитори.

2. Обхват

2.1. Настоящата политика се прилага за всички компоненти на ИТ мрежата на организацията, включително:

2.1.1. Кабелна и безжична инфраструктура в офис локациите

2.1.2. Маршрутизатори, комутатори, точки за достъп, защитни стени и шлюзове

2.1.3. Връзки за отдалечен достъп, включително VPN, RDP и облачни тунели

2.1.4. Облачни приложения, достъпвани от вътрешни или външни мрежи

2.1.5. Устройства, свързани към мрежата от служители, външни изпълнители или гости

2.2. Настоящата политика урежда както физическите, така и логическите мрежови сегменти, включително гостови зони, IoT устройства и вътрешноадминистративни системи.

2.3. Политиката обхваща целия персонал с достъп до мрежата на организацията, включително:

2.3.1. Вътрешни служители

2.3.2. Лица, работещи дистанционно, и хибридно работещ персонал

2.3.3. Външни доставчици, консултанти и външни доставчици на услуги

2.3.4. Гости, използващи временен Wi-Fi достъп

3. Цели

3.1. Да се гарантира, че мрежата на организацията е защитена срещу неразрешен достъп и външни киберзаплахи

3.2. Да се осигури правилно сегментиране между доверени и недоверени мрежи (напр. Wi-Fi за гости, достъп на доставчици)

3.3. Да се осигури сигурна отдалечена свързаност без компрометиране на вътрешните системи

3.4. Да се предотвратяват разпространението на зловреден софтуер и извличането на данни чрез мрежови канали

3.5. Да се осигурят мониторинг, предупреждения и одитни записи на мрежовата активност в подкрепа на откриването на инциденти и съответствието

3.6. Да се гарантира, че само одобрени и защитени устройства могат да се свързват към вътрешните мрежи

3.7. Да се изпълняват задълженията по ISO 27001, GDPR и свързаните рамки за киберсигурност

4. Роли и отговорности

4.1. Управител

4.1.1. Отговаря за настоящата политика и гарантира, че са осигурени подходящи ресурси за сигурно проектиране и управление на мрежата

4.1.2. Преглежда изключенията от контролите за мрежова сигурност и одобрява споразуменията за мрежов достъп на доставчици

4.1.3. Преглежда инциденти или одитни констатации, свързани със слабости в мрежовата сигурност

4.2. Външен доставчик на ИТ поддръжка / вътрешна ИТ функция

4.2.1. Внедрява, конфигурира и поддържа всички защитни стени, маршрутизатори, комутатори и безжични контролери

4.2.2. Управлява сегментирането между вътрешни, гостови и външни мрежи

4.2.3. Наблюдава журналите и автоматичните предупреждения за опити за неразрешен достъп или мрежови аномалии

4.2.4. Гарантира, че актуализациите на фърмуера и конфигурацията се прилагат сигурно и своевременно

[... 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. Годишен преглед

9.1.1. Настоящата политика трябва да се преглежда най-малко веднъж годишно от Управителя съвместно с външния доставчик на ИТ поддръжка и координатора по поверителност.

9.2. Основания за междинен преглед

9.2.1. Преглед на политиката трябва да се инициира и при:

9.2.1.1. Съществени промени в мрежовата архитектура (напр. нови VPN или системи за защитни стени)

9.2.1.2. Инцидент, свързан с мрежата (напр. проникване, разпространение на ransomware или извличане на данни)

9.2.1.3. Правни, регулаторни или рамкови актуализации, засягащи защитата на мрежата

9.2.1.4. Нови платформи на доставчици, изискващи алтернативни методи за достъп или протоколи

9.3. Управление на версиите и документация

9.3.1. Ревизиите на политиката трябва да се документират с номер на версия, дата и обобщение на промените

9.3.2. Предходните версии трябва да се архивират за срок не по-малък от 3 години

9.3.3. Актуализациите трябва да се комуникират на засегнатите служители, като се изисква потвърждение за запознаване, когато се въвеждат съществени промени в изискваното поведение

10. Свързани политики и връзки

10.1. Настоящата политика трябва да се прилага съвместно със следните политики за сигурност за SME:

10.1.1. P9S – Политика за дистанционна работа: Налага сигурни методи за отдалечен достъп, изисквания за VPN и защита на крайните точки за потребители извън обекта.

10.1.2. P12S – Политика за управление на активите: Гарантира, че всички системи, свързани към мрежата, са идентифицирани, категоризирани и проследявани с актуален статус на сигурност.

10.1.3. P17S – Политика за защита на данните и поверителност: Гарантира, че мрежовата сегментация, контролът на достъпа и журналирането подпомагат принципите за поверителност и защита на данните по GDPR.

10.1.4. P22S – Политика за регистриране и мониторинг: Определя изискванията за събиране и преглед на журнали от мрежови устройства, отдалечени връзки и безжични контролери.

10.1.5. P30S – Политика за реагиране при инциденти: Определя необходимите действия при нарушения на мрежата, опити за неразрешен достъп или разпространение на зловреден софтуер чрез вътрешни мрежи.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 8.1 – Изисква прилагане на контроли за осигуряване на сигурни и устойчиви операции, включително за мрежите.

11.2. ISO/IEC 27002

11.2.1. Контрол 8.20 – Предоставя технически и процедурни насоки за защита на мрежовия достъп, сегментиране на мрежата и мониторинг.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Изисква контрол върху потока на информация в мрежите и между системите.

11.3.2. SC-7 – Изисква защита на границите, сигурна маршрутизация и сегментиране на мрежата за намаляване на риска от неразрешен достъп.

11.4. GDPR на ЕС

11.4.1. Член 32 – Изисква подходящи технически и организационни мерки за гарантиране на поверителността, цялостта и наличността на мрежово свързаните системи и услуги, които обработват лични данни.

11.5. Директива NIS2 на ЕС

11.5.1. Член 21(2)(d) – Изисква технически мерки, базирани на риска, включително мрежова сигурност и контрол на достъпа.

11.5.2. Член 21(2)(e) – Изисква сегментиране и изолация на системите, за да се предотврати разпространението на киберинциденти.

11.6. DORA на ЕС

11.6.1. Член 9 – Изисква организациите да прилагат контроли за управление на ИКТ риска, включително за сигурни мрежи и комуникации.

11.6.2. Член 10 – Изисква стратегиите за цифрова устойчивост да обхващат защитата на мрежовата инфраструктура и отдалечената свързаност.

11.7. COBIT 2019

11.7.1. DSS05.02 – Изисква ефективна защита на ИТ инфраструктурата и мрежовите среди срещу вътрешни и външни заплахи.

11.7.2. APO13.01 – Изисква стратегии за управление на риска, които включват сегментиране на мрежата и мониторинг като част от смекчаването на заплахите.