					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P21					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**

Съгласуване със стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	Неприложимо
ISO/IEC 27002:2022	Контроли 8.20-8.22	Неприложимо
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	Неприложимо
GDPR на ЕС	Член 32	Неприложимо
NIS2 на ЕС	Член 21(2)(d)	Неприложимо
DORA на ЕС	Член 9	Неприложимо
COBIT 2019	DSS01.03, DSS05.01, MEA03	Неприложимо

1. Цел

1.1 Целта на тази политика е да определи изискванията на организацията за защита на нейните вътрешни и външни мрежи от неоторизиран достъп, прекъсване на услуги, прихващане на данни и неправомерно използване.

1.2 Тя гарантира, че цялата мрежова инфраструктура — включително физическа, виртуална, облачна и хибридна — е защитена чрез многостепенна защита, включително сегментиране на мрежата, прилагане на правила на защитни стени, сигурно маршрутизиране и централизиран мониторинг.

1.3 Настоящата политика прилага изискванията на ISO/IEC 27001, клауза 8.1, и контролите от Приложение A 8.20 до 8.22, като осигурява съответствие с приложимите правни и регулаторни задължения по GDPR, член 32, NIS2, член 21, и DORA, член 9.

2. Обхват

2.1 Настоящата политика се прилага за всички мрежи и свързаните с тях инфраструктурни компоненти, включително:

2.1.1 маршрутизатори, комутатори, безжични точки за достъп и защитни стени

2.1.2 облачни виртуални мрежи (напр. AWS VPC, Azure VNet), VPN концентратори и SD-WAN системи

2.1.3 вътрешни LAN мрежи, DMZ зони, канали за отдалечен достъп и връзки между обекти или с трети страни

2.1.4 поддържащи системи, като DNS, DHCP, прокси сървъри и средства за мониторинг

2.2 Политиката е задължителна за целия персонал и външните доставчици на услуги, които управляват, конфигурират, наблюдават или взаимодействат с мрежите на организацията, независимо дали са в локалната инфраструктура или в облака.

2.3 Всички системи и приложения, свързани към мрежите на организацията — независимо от местоположението или собствеността им — трябва да отговарят на тези изисквания за мрежова сигурност.

3. Цели

3.1 Да се гарантират поверителността, целостта и наличността на данните, предавани по мрежите, чрез ефективен контрол на достъпа, сигурно маршрутизиране и мониторинг.

3.2 Да се предотвратяват неоторизиран достъп, странично придвижване и злоупотреба с мрежови ресурси чрез прилагане на сегментиране на мрежата, зониране и защита на периметъра.

3.3 Да се поддържат последователни мрежови конфигурации въз основа на добри практики в индустрията и информация за заплахи с цел защита срещу развиващи се киберрискове.

3.4 Да се защитават външните комуникации, облачната свързаност и отдалеченият достъп чрез криптирани канали, стриктна автентикация и валидиране на крайните точки.

3.5 Да се осигурява видимост върху мрежовата активност чрез централизирано регистриране на събития, инспекция на трафика в реално време и автоматизирани предупреждения.

3.6 Да се осигури регулаторно съответствие чрез привеждане на всички мрежови операции в съответствие с изискванията на ISO/IEC 27001:2022, GDPR, NIS2, DORA и COBIT 2019.

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO)

4.1.1 Отговаря за настоящата политика и осигурява нейния преглед и съгласуване с цялостната стратегия на организацията за киберсигурност.

4.1.2 Одобрява моделите за сегментиране на мрежата, наборите от правила на защитните стени за чувствителни системи и исканията за изключения.

4.2 Мениджър по мрежова сигурност / Ръководител по сигурността на инфраструктурата

4.2.1 Управлява архитектурата за мрежова защита, включително защитни стени, системи за откриване/предотвратяване на проникване (IDS/IPS), VPN и сигурно маршрутизиране.

4.2.2 Осъществява надзор върху сегментирането на мрежата, присвояването на VLAN, зонирането на трафика и външната свързаност.

4.2.3 Осигурява текущ преглед на филтрирането на входящия и изходящия трафик и прилагането на Zero Trust на всички мрежови нива.

[... 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 Настоящата политика подлежи на годишен преглед от Мениджъра по мрежова сигурност в сътрудничество с Директора по информационна сигурност (CISO) и се актуализира въз основа на:

9.1.1 нововъзникващи заплахи (напр. нови техники за атака, уязвимости в протоколи)

9.1.2 промени в инфраструктурата (напр. миграции към облака, внедряване на SD-WAN)

9.1.3 регулаторни актуализации или актуализации на стандарти, засягащи мрежовата защита

9.1.4 одитни констатации, тенденции при инцидентите или влошаване на резултатността, причинено от контролите

9.2 Прегледите трябва да се задействат и при:

9.2.1 съществени промени в мрежовата архитектура

9.2.2 внедряване на нови платформи за защитни стени, VPN или облачни мрежи

9.2.3 извеждане от употреба на ключови активи или доверени зони

9.3 Актуализациите трябва да се регистрират в регистъра за контрол на документи на СУИС и да се разпространяват до:

9.3.1 екипите по инфраструктура и мрежови операции

9.3.2 екипите на SOC и инженерите по сигурността

9.3.3 екипите по приложения с зависимости от мрежови потоци

9.3.4 всички доставчици от трети страни с активна взаимосвързаност

9.4 Всички предходни версии на политиката трябва да се архивират сигурно с анотации към историята на промените, за да се запазят възможността за одит и проследимостта на промените.

10. Свързани политики и връзки

10.1 P1 - Политика за информационна сигурност. Установява основните принципи за сигурност и изисква многостепенна защита, включително мрежово базирани контроли за достъп и защита от заплахи.

10.2 P4 - Политика за контрол на достъпа. Гарантира, че сегментирането на мрежата се прилага в съответствие с потребителските роли, принципа на минималните привилегии и правилата за предоставяне на достъп.

10.3 P5 - Политика за управление на промените. Регламентира промените по защитните стени, корекциите на VPN правила и промените в маршрутизирането чрез документиран процес с възможност за одит.

10.4 P12 - Политика за управление на активите. Подпомага идентифицирането и класификацията на мрежово свързаните системи и гарантира, че всички свързани активи се управляват в рамките на определените от политиката обхвати.

10.5 P22 - Политика за регистриране и мониторинг. Регламентира събирането, корелацията и съхранението на мрежови журнали, включително събития от защитни стени, опити за достъп и открити аномалии.

10.6 P30 - Политика за реагиране при инциденти. Определя процедурите за ескалация, ограничаване и отстраняване в отговор на мрежови заплахи или прониквания, като DDoS, странично придвижване или неоторизиран достъп.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международни стандарти и регулаторни изисквания, които определят сигурни мрежови операции, сегментиране на мрежата, защита на периметъра и сигурен отдалечен достъп.

11.2 ISO/IEC 27001

11.2.1 Клауза 8.1 - Оперативно планиране и контрол: Изисква техническите контроли, включително мерките за мрежова защита, да бъдат интегрирани в оперативните процеси.

11.3 ISO/IEC 27002:2022

11.3.1 Контроли 8.20-8.22: Предоставят насоки за защита на мрежите, сегментиране на услуги и защита на мрежовите услуги чрез контрол на достъпа и мониторинг.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Защита на границите: Изисква периметрови контроли, сегментиране на мрежата и сигурни взаимосвързвания.

11.4.2 AC-4 - Прилагане на контрол върху информационните потоци: Подпомага зонирането и ограниченията на трафика, базирани на правила.

11.4.3 SC-32 - Разделяне на информационни системи: Насърчава логическото разделяне на информационните системи.

11.5 GDPR на ЕС (2016/679)

11.5.1 Член 32 - Сигурност на обработването: Изисква технически мерки — като защитни стени и сегментиране на мрежата — за защита на личните данни.

11.6 Директива NIS2 на ЕС (2022/2555)

11.6.1 Член 21(2)(d): Изисква ефективна сигурност на мрежите и информационните системи, защита на периметъра, сигурна конфигурация и контроли за разделяне.

11.7 DORA на ЕС (2022/2554)

11.7.1 Член 9 - Управление на ИКТ риска: Задължава финансовите субекти да защитават мрежите и взаимосвързаността от неоторизиран достъп, изтичане на данни и оперативни смущения.

11.8 COBIT 2019

11.8.1 DSS01.03 - Наблюдение на инфраструктурата: Изисква проактивен контрол върху техническото състояние и свързаността на мрежата.

11.8.2 DSS05.01 - Защита срещу зловреден софтуер: Включва сегментиране на мрежата и защита на периметъра за ограничаване на разпространението.

11.8.3 MEA03 - Мониторинг, оценяване и преценка на съответствието: Укрепва прилагането на мрежовата политика и оценките на съответствието.