					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P35S					Заглавие на документа: **Политика за сигурност на IoT / OT**							
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**

Съответствие със стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.1, 6.2, 8	
ISO/IEC 27002:2022	Контроли 5.23, 5	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
GDPR на ЕС	Член 32	
NIS2 на ЕС	Член 21(2)(a), (d), (f)	
DORA на ЕС	Член 9(2), 10(1)	

1. Цел

1.1. Настоящата политика определя задължителните правила за сигурно използване и управление на устройства от интернет на нещата (IoT) и оперативни технологии (OT) в рамките на организацията. Тези устройства могат да включват интелигентни сензори, камери за сигурност, производствени машини, контролери за HVAC или други индустриални системи, свързани към мрежа.

1.2. Целта на тази политика е да:

1.2.1. Защитава физическите и цифровите операции от прекъсване или манипулиране чрез недостатъчно защитени свързани устройства

1.2.2. Осигурява безопасно внедряване, наблюдение и поддръжка на IoT и OT системи

1.2.3. Осигурява съответствие с ISO/IEC 27001:2022, Директива NIS2 и свързаните регулаторни рамки

1.2.4. Предоставя практически и приложими контроли за МСП, работещи в офисна, складова или производствена среда

2. Обхват

2.1. Тази политика се прилага за всички лица, участващи в планирането, инсталирането, конфигурирането, използването, поддръжката или извеждането от употреба на IoT или OT устройства. Това включва:

2.1.1. Служители, външни изпълнители или стажанти с физически или отдалечен достъп до устройства

2.1.2. Доставчици от трети страни или сервизни техници, които инсталират или поддържат свързани системи

2.1.3. Ръководители или служители, отговорни за надзора върху политиките за сигурност

2.2. Политиката обхваща:

2.2.1. IoT устройства като интелигентни брави, системи за видеонаблюдение, интелигентни измервателни уреди или принтери

2.2.2. OT системи, включително PLC (програмируеми логически контролери), SCADA панели или индустриални шлюзове

2.2.3. Поддържащия хардуер, приложенията за управление и комуникационните мрежи, използвани от тези системи

2.3. Тази политика се прилага за всички работни локации: офисни среди, отдалечени обекти, производствени помещения и облачни платформи, които взаимодействат с тези устройства.

3. Цели

3.1. Сигурно внедряване: Да се гарантира, че всички IoT/OT системи са сигурно конфигурирани преди въвеждането им в експлоатация.

3.2. Ограничаване на експозицията: Да се предотвратят неоторизиран достъп, неправомерно използване или компрометиране на свързани устройства чрез прилагане на надежден контрол на достъпа и мрежова сегментация.

3.3. Непрекъснато наблюдение: Да се поддържа видимост върху IoT/OT операциите чрез регистриране на дейностите и наблюдение за необичайно поведение.

3.4. Отчетност на доставчиците: Да се гарантира, че външните доставчици спазват практики за сигурно инсталиране, конфигуриране и поддръжка.

3.5. Регулаторно съответствие: Да се демонстрира пълно съответствие с приложимите стандарти като ISO 27001, GDPR (ако се събират лични данни) и NIS2 за устойчивост на критичната инфраструктура.

4. Роли и отговорности

4.1. Управител

4.1.1. Носи цялостна отговорност за сигурността на IoT и OT системите

4.1.2. Одобрява тази политика и гарантира нейното прилагане във всички работни зони

4.1.3. Проверява, че доставчиците и външните изпълнители спазват практики за сигурно внедряване и поддръжка

4.1.4. Оторизира мрежовия достъп за всяка IoT/OT система

4.2. Определен служител или оперативен ръководител (ако е назначен)

4.2.1. Осъществява надзор върху инвентара, внедряването и конфигурирането на IoT/OT устройствата

4.2.2. Регистрира местоположението на всяко устройство, неговото мрежово предназначение и документацията за поддръжка

4.2.3. Гарантира, че всички промени (напр. актуализации на фърмуера или подмяна на устройства) са документирани

[... 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. Тази политика трябва да се преглежда най-малко веднъж годишно от Управителя

9.1.2. Прегледът трябва да оцени дали политиката остава ефективна, обхваща актуалните типове устройства и съответства на новите рискове или технологии

9.2. Актуализации при настъпване на събитие

9.2.1. Актуализации на политиката трябва също да се инициират, когато:

9.2.2. Бъдат въведени нови типове IoT или OT системи

9.2.3. Доставчиците издадат бюлетини по сигурността или уведомления за край на жизнения цикъл

9.2.4. Инцидент или одит идентифицира пропуски в контролите за IoT/OT

9.2.5. Нови закони или стандарти наложат допълнителни изисквания

9.3. Документиране и управление на версиите

9.3.1. Всички актуализации трябва да бъдат документирани, включително дата, номер на версията и обобщение на промените

9.3.2. Управителят трябва да съхранява историческите версии на политиката за целите на одит

9.4. Комуникиране на промените

9.4.1. Всички актуализации на политиката трябва да бъдат споделяни с всички относими служители и доставчици

9.4.2. Актуализираните версии трябва да бъдат достъпни чрез споделени папки или печатни материали на местата за инсталиране или в контролните центрове

10. Свързани политики и връзки

10.1. Тази политика трябва да се прилага в съответствие със следните свързани политики за МСП:

10.1.1. P4S – Политика за контрол на достъпа: Налага контроли за достъп на ниво устройство, използване на силни пароли и процедури за оторизиран достъп до IoT и OT платформи

10.1.2. P9S – Политика за дистанционна работа: Предотвратява използването на отдалечен достъп до IoT/OT табла за управление чрез несигурни или неодобрени канали

10.1.3. P17S – Политика за защита на данните и поверителност: Прилага се, ако IoT устройства (напр. камери за сигурност) обработват или записват лични данни, като осигурява съответствие с GDPR

10.1.4. P30S – Политика за реагиране при инциденти: Определя процедурите за откриване, докладване и отстраняване на IoT или OT инциденти, включително предполагаема манипулация или оперативен отказ

10.1.5. P36S – Политика за социални медии и външни комуникации: Гарантира, че информация за устройства или мрежова схема не се споделя външно без одобрение

10.2. Всяка свързана политика укрепва прилагането и практическото използване на тази политика чрез целеви процедурни указания.

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Клауза 6.1 – Идентифициране и третиране на риска: Изисква рисковете, свързани с IoT и OT системите, да бъдат систематично оценявани и смекчавани

11.1.2. Клауза 8.1 – Оперативно планиране и контрол: Осигурява сигурен оперативен контрол върху свързаните устройства

11.2. ISO/IEC 27002

11.2.1. Контрол 5.23 – Информационна сигурност при използване на оперативни технологии: Определя сигурното използване на OT във физически и цифрови среди

11.2.2. Контрол 5.31 – Сигурна конфигурация на информационните системи: Изисква укрепени конфигурации за IoT/OT устройства и избягване на несигурни настройки по подразбиране

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – Цялостност на софтуера, фърмуера и информацията: Изисква валидиране на целостта на фърмуера и актуализациите

11.3.2. CM-7 – Минимална функционалност: Устройствата не трябва да имат активирани неизползвани или несигурни функции

11.3.3. AC-6 – Минимални привилегии: Достъпът до устройствата трябва да бъде ограничен само до оторизирани потребители

11.3.4. PE-20 – Мониторинг на активи: Физически и оперативен мониторинг на IoT и OT активи

11.3.5. SC-7 – Защита на границите: Сегментиране и контрол на мрежовите комуникации за свързани системи

11.4. GDPR на ЕС (2016/679)

11.4.1. Член 32 – Сигурност на обработването: Ако се събират лични данни (напр. чрез камери за видеонаблюдение), организацията трябва да прилага подходящи технически и организационни мерки за защита на това обработване

11.5. Директива NIS2 на ЕС (2022/2555)

11.5.1. Член 21(2)(a) – Мерки за управление на риска

11.5.2. Член 21(2)(d) – Сигурна конфигурация и използване на устройства

11.5.3. Член 21(2)(f) – Сигурност на веригата на доставки и системите

11.6. DORA на ЕС (2022/2554)

11.6.1. Член 9(2) – Обхват на управлението на ИКТ риска: Включва индустриални и вградени устройства, използвани в оперативни среди

11.6.2. Член 10(1) – Непрекъсваемост на ИКТ: Изисква конфигурациите на устройствата да поддържат устойчивост и дейности по възстановяване

11.7. COBIT 2019

11.7.1. DSS01 – Управление на операциите: Прилага се за надзора върху технологичните операции, включително физически устройства

11.7.2. DSS05 – Управление на услугите по сигурност: Гарантира, че свързаните системи са надлежно наблюдавани и защитени

11.7.3. APO13 – Управление на сигурността: Подсилва политиките за защита на оперативните активи в рамките на МСП