					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P35					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**

Съгласувано с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 8	
ISO/IEC 27002:2022	Контроли 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
GDPR на ЕС	Членове 5, 25, 32	
NIS2 на ЕС	Членове 21, 23	
DORA на ЕС	Членове 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Цел

1.1 Настоящата политика определя задължителните изисквания за информационна сигурност при внедряването, експлоатацията, наблюдението и извеждането от употреба на системи от тип Internet of Things (IoT) и Operational Technology (OT) в рамките на организацията.

1.2 Тя гарантира, че тези системи са интегрирани в общата система за управление на киберсигурността на организацията и са защитени срещу компрометиране, неразрешено използване и саботаж на операциите.

1.3 Политиката има за цел да наложи надеждни технически, организационни и процедурни контроли за защита на IoT/OT системи, които взаимодействат с физическа инфраструктура, производствени процеси и среди с критично значение за безопасността.

1.4 Тя подпомага изпълнението на регулаторните и договорните задължения в областта на киберсигурността, безопасността, екологичния контрол и непрекъсваемостта на дейността.

2. Обхват

2.1 Настоящата политика се прилага за всички IoT и OT системи — независимо дали са собственост на дружеството, наети или предоставени от трети страни — използвани в оперативната, административната или производствената среда на организацията.

2.2 Обхванатите системи включват, без изброяването да е изчерпателно:

2.2.1 IoT устройства, като сензори за околна среда, системи за контрол на достъпа, интелигентно осветление, оборудване за видеонаблюдение и носими устройства

2.2.2 OT платформи, като PLC, SCADA, DCS, HMI панели, MES интерфейси и полеви контролери

2.2.3 Индустриални мрежи за управление или активи, свързани с облачни услуги, които наблюдават физически операции

2.3 Политиката обхваща:

2.3.1 Всички среди (локални, периферни и управлявани от облака)

2.3.2 Всички заинтересовани страни (вътрешни потребители, интегратори, външни доставчици, изпълнители)

2.3.3 Всички етапи от жизнения цикъл (проектиране, снабдяване, внедряване, експлоатация, извеждане от употреба)

3. Цели

3.1 Да се защити IoT и OT инфраструктурата от вътрешни и външни киберзаплахи, включително отказ от услуга, неразрешен достъп, разпространение на рансъмуер и манипулиране на фърмуер.

3.2 Да се гарантира, че IoT/OT платформите не се превръщат във вектор за атака през границата между IT и OT, нито в средство за компрометиране на системи с критично значение за безопасността.

3.3 Да се прилагат принципите „сигурност още при проектиране“ и многостепенна защита през целия жизнен цикъл на тези технологии.

3.4 Да се осигури надеждна, сигурна и подлежаща на одит интеграция на IoT и OT платформите в центъра за операции по сигурността (SOC) на организацията и в плановете за реагиране при инциденти.

3.5 Да се гарантира, че всички внедрявания са съгласувани с контролите по ISO/IEC 27001 и приложимите секторни насоки (напр. IEC 62443, ISO/IEC 27019, NIST SP 800-82).

4. Роли и отговорности

4.1 Директор по информационна сигурност (CISO) / Ръководител по информационна сигурност

4.1.1 Определя политиките и техническите стандарти за киберсигурност на IoT/OT.

4.1.2 Осъществява надзор върху оценките на риска, валидирането на контролите и координацията между отделите.

4.2 OT инженери / Ръководители на обекти и производствени звена

4.2.1 Валидират конфигурациите на OT системите и осигуряват спазването на политиката в производствените зони.

4.2.2 Поддържат физическите и логическите мерки за защита на целостта и безопасността на OT средата.

[... 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 Настоящата политика трябва да се преглежда най-малко веднъж годишно и да се актуализира въз основа на:

9.1.1 Промени в архитектурата, доставчиците или платформите на OT или IoT системите

9.1.2 Съществени регулаторни промени (напр. изменения в DORA, NIS2, секторни директиви)

9.1.3 Поява на нови уязвимости или модели на заплахи в системите за управление

9.1.4 Констатации от вътрешни или външни одити, тестове за проникване или red team упражнения

9.2 CISO, Ръководителят по сигурността на OT и ръководителите на съответните отдели носят съвместна отговорност за иницииране на процеса по преглед.

9.3 Извънредни прегледи трябва да се инициират след:

9.3.1 Всеки инцидент, свързан с IoT/OT, довел до отказ на система или загуба на данни

9.3.2 Въвеждане на съществено ново оборудване, софтуер за наблюдение или платформи за фърмуер

9.3.3 Интегриране на интелигентни периферни изчисления или автоматизация с AI на полево ниво

9.4 Всички промени по политиката трябва да бъдат:

9.4.1 Документирани в историята на версиите и в Регистъра на промените по политики

9.4.2 Комуникирани до всички засегнати потребители, доставчици и IT/OT оператори

9.4.3 Одобрени повторно от изпълнителното ръководство

10. Свързани политики и връзки

10.1 Настоящата политика функционира съвместно със следните политики по информационна сигурност и се подпомага от тях:

10.1.1 P1 – Политика по информационна сигурност: Установява основополагащи принципи за сигурност, които се прилагат и към сигурността на IoT и OT системите.

10.1.2 P3 – Политика за приемлива употреба: Определя ограниченията върху използването на лични и неразрешени устройства, включително в оперативна среда.

10.1.3 P6 – Политика за управление на риска: Насочва оценката, приемането и ограничаването на рискове, свързани с вградени системи и системи за управление.

10.1.4 P12 – Политика за управление на активите: Гарантира, че всички IoT и OT системи са формално инвентаризирани и са определени отговорни собственици.

10.1.5 P20 – Политика за защита на крайни устройства / злонамерен софтуер: Прилага се към свързани контролери, интелигентни шлюзове и периферни системи в производството.

10.1.6 P22 – Политика за журнализиране и наблюдение: Разпростира се върху процедурите за събиране и преглед на журнали в OT среди.

10.1.7 P30 – Политика за реагиране при инциденти: Пряко урежда начина, по който нарушения, аномалии или откази на системи, свързани с IoT/OT, трябва да бъдат ескалирани и управлявани.

10.1.8 P33 – Политика за одит и наблюдение на съответствието: Осигурява механизми за потвърждаване на текущото съответствие с настоящата политика.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати стандарти и регулаторни рамки, които гарантират сигурността, устойчивостта и съответствието на системите Internet of Things (IoT) и Operational Technology (OT) в индустриална, производствена и корпоративна среда.

11.2 ISO/IEC 27002:2022 – Контроли 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Контрол 5.7 – Разузнаване за заплахи: Подпомага наблюдението на OT среди и идентифицирането на специфични за IoT уязвимости.

11.2.2 Контрол 5.23 – Информационна сигурност при използване на облачни услуги: Прилага се, когато IoT устройства взаимодействат с облачни платформи за телеметрия, управление или анализ.

11.2.3 Контрол 5.27 – Сигурна архитектура на системите и инженерни принципи: Регламентира принципите за сигурност още при проектиране за вградени системи и мрежи за управление.

11.2.4 Контрол 5.31 – Сигурност в процесите по разработка и поддръжка: Налага валидиране на софтуер и фърмуер, контроли върху кръпките и изисквания към доставчиците при OT внедрявания.

11.2.5 Контрол 5.36 – Съответствие със законови и договорни изисквания: Гарантира съответствието на OT активите с изискванията за безопасност, околна среда и регулаторните изисквания.

11.2.6 Тези контроли съвместно установяват добри практики за защита на IoT/OT системите през целия им жизнен цикъл, включително проектиране на архитектурата, сигурно

внедряване, управление на кръпки, откриване на аномалии и съответствие със секторните изисквания.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Защита на границите: Гарантира, че OT мрежите са сегментирани и защитени от неразрешен достъп.

11.3.2 SI-4 – Наблюдение на системите: Изисква внедряване на механизми за непрекъснато наблюдение и откриване на аномалии в ICS среди.

11.3.3 CM-2 – Базова конфигурация: Налага контрол върху конфигурациите и укрепване на IoT/OT платформите.

11.3.4 AC-6 – Минимални привилегии: Прилага се за потребителския достъп и отдалеченото обслужване от доставчици на вградени системи за управление.

11.3.5 PL-8 – Архитектури за сигурност и поверителност: Регламентира планирането на сигурната интеграция на системите, особено при проекти за модернизация на OT.

11.4 GDPR на ЕС (2016/679)

11.4.1 Член 5 – Принципи, свързани с обработването на лични данни: Прилага се към IoT платформи, които обработват базирани на сензори или поведенчески данни, свързани с физически лица.

11.4.2 Член 25 – Защита на данните още при проектирането и по подразбиране: Изисква мерки за защита на личните данни, вградени в дизайна на IoT продукти и фърмуер.

11.4.3 Член 32 – Сигурност на обработването: Налага криптиране, контрол на достъпа и сигурни комуникации при предаване на данни от интелигентни устройства.

11.5 Директива NIS2 на ЕС (2022/2555)

11.5.1 Членове 21 и 23: Налагат задължения по сигурността за съществени и важни субекти, които използват OT системи. Те включват оценка на риска, докладване на инциденти и валидиране на доставчиците на IoT/OT и на целостта на фърмуера по веригата на доставки.

11.6 DORA на ЕС (2022/2554)

11.6.1 Член 9 – Управление на ИКТ риска: Изисква сигурна интеграция на вградени системи и OT технологии в програмата за управление на ИКТ риска.

11.6.2 Член 10 – Изисквания за сигурност на ИКТ: Налага защитни мерки за взаимосвързани OT платформи, използвани във финансова среда и среди на критични услуги.

11.7 COBIT 2019

11.7.1 DSS05.01 – Защита срещу злонамерен софтуер: Включва откриване и реакция при специфични за ICS заплахи и кампании със зловреден софтуер, насочени към IoT.

11.7.2 BAI09.01 – Установяване и поддържане на изисквания за сигурност: Съответства на сигурното осигуряване и експлоатация на интелигентна или вградена инфраструктура.

11.7.3 APO13.02 – Установяване и поддържане на план за информационна сигурност: Изисква включването на OT системите и техните уязвимости в общата стратегия на организацията за киберсигурност.