					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P04S					Заглавие на документа: **Политика за контрол на достъпа**							
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, когато е приложимо

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 5	
ISO/IEC 27002:2022	Контроли: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 до AC-5	
GDPR на ЕС	Член 32	
NIS2 на ЕС	Член 21(2)(b)	
DORA на ЕС	Член 9	
COBIT 2019	APO07, DSS01	

1. Цел

1.1. Настоящата политика определя как организацията управлява достъпа до системи, данни и обекти, така че само упълномощени лица да имат достъп до информация въз основа на служебна необходимост.

1.2. Политиката установява ясни правила за предоставяне, промяна, наблюдение и отнемане на потребителски достъп с цел минимизиране на риска от неразрешен достъп и подпомагане на съответствието с приложимите закони и стандарти.

1.3. Политиката въвежда принципа на най-малките привилегии, като изисква достъпът да бъде ограничен до минимално необходимото за изпълнение на служебните задължения.

2. Обхват

2.1. Настоящата политика се прилага за всички лица, които използват или управляват достъп до ИТ системите, мрежите, данните или обектите на организацията, включително:

2.1.1. Служители

2.1.2. Изпълнители по договор

2.1.3. Временни служители

2.1.4. Външни доставчици на ИТ услуги

2.2. Политиката обхваща достъп до:

2.2.1. Корпоративни приложения, споделени файлови ресурси и бази данни

2.2.2. Електронна поща, VPN и системи за отдалечен достъп

2.2.3. Облачни услуги, използвани за бизнес цели

2.2.4. Физически достъп до защитени обекти, като офиси или сървърни помещения

2.3. Настоящата политика се прилага за всички устройства (предоставени от дружеството или одобрени по BYOD), платформи и местоположения.

3. Цели

3.1. Да се гарантира, че права за достъп се предоставят само след официално одобрение въз основа на роля и бизнес обосновка.

3.2. Да се предотврати неразрешен или прекомерен достъп до чувствителни данни, системи или инфраструктура.

3.3. Да се определят ясни процедури за предоставяне, промяна и прекратяване на потребителски достъп.

3.4. Да се изискват редовни прегледи на достъпа и автоматизирано или ръчно водене на журнали в подкрепа на одитни дейности.

3.5. Да се подпомогне техническото прилагане на ограниченията за достъп чрез конфигуриране и наблюдение.

4. Роли и отговорности

4.1. Управител

4.1.1. Одобрява настоящата политика и осигурява необходимите ресурси за прилагане на ефективни контроли за достъп.

4.1.2. Одобрява изключенията и преглежда годишните одити на достъпа.

4.2. ИТ мениджър / външен доставчик на ИТ услуги

4.2.1. Отговаря за създаването, промяната и закриването на потребителски акаунти.

4.2.2. Поддържа регистър за контрол на достъпа, съдържащ всички дейности (създаване, промяна, премахване).

4.2.3. Прилага контрол на достъпа, базиран на роли (RBAC), и налага използването на силна автентикация (напр. MFA).

4.2.4. Преглежда журналите за достъп за подозрителна активност и докладва установените проблеми на управителя.

[... 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 на политиката

9.1.1. ИТ мениджърът трябва да преглежда настоящата политика ежегодно. Всяка промяна в правния, техническия или организационния контекст трябва да води до незабавна актуализация.

9.2. Основания за преглед

9.2.1. Политиката трябва да бъде прегледана и при настъпване на някое от следните обстоятелства:

9.2.2. Съществени промени в системите или миграции към облачни услуги

9.2.3. Промени в ролите или организационната структура

9.2.4. Инцидент по информационна сигурност, включващ неразрешен достъп

9.2.5. Регулаторни промени (напр. актуализации по GDPR, NIS2 или DORA)

9.3. Документиране и съобщаване на промените

9.3.1. Промените трябва да се документират с история на версиите, одобрение от управителя и да се довеждат до знанието на всички засегнати лица.

9.4. Достъпност и обучение

9.4.1. Настоящата политика трябва да бъде предоставена на всички служители, а съответното обучение следва да бъде част от първоначалното въвеждане и да се провежда ежегодно след това.

10. Свързани политики и взаимовръзки

10.1. Настоящата политика следва да се прилага съвместно със следните политики за МСП с цел цялостно прилагане на практиките за сигурен достъп:

10.1.1. P3S – Политика за допустимо използване: Гарантира, че потребителите разбират допустимото поведение при предоставен достъп.

10.1.2. P5S – Политика за управление на промените: Гарантира, че правата за достъп са съобразени с одобрените промени по системите.

10.1.3. P7S – Политика за въвеждане и прекратяване: Определя събитията, които задействат предоставяне и отнемане на потребителски достъп.

10.1.4. P17S – Политика за защита на данните и поверителност: Гарантира, че контролите за достъп са съобразени със защитата на личните данни.

10.1.5. P30S – Политика за реакция при инциденти: Определя как се управляват и разследват инциденти, свързани с достъпа (напр. неправомерно използване или пробиви).

11. Референтни стандарти и рамки

11.1. ISO/IEC 27001

11.1.1. Контрола 5.15 – Изисква формализирани политики и процеси за контрол на достъпа.

11.2. ISO/IEC 27002

11.2.1. Контроли 5.15–5.17 – Определят подробни насоки за достъп, базиран на роли, управление на жизнения цикъл на потребителите и управление на привилегирован достъп.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 до AC-5 – Изискват структурирани политики за управление на достъпа, включително упълномощаване на акаунти, преглед и наблюдение.

11.4. GDPR на ЕС

11.4.1. Член 32 – Изисква технически и организационни контроли (като управление на достъпа), за да се гарантират сигурността и поверителността на данните.

11.5. Директива NIS2 на ЕС

11.5.1. Член 21(2)(b) – Изисква оперативен контрол на достъпа и системи за управление на идентичността с цел предотвратяване на неразрешен достъп до системи.

11.6. DORA на ЕС

11.6.1. Член 9 – Подчертава необходимостта от сигурно управление на ИКТ рисковете, включително надежден контрол на достъпа за финансовите субекти.

11.7. COBIT 2019

11.7.1. APO07 – Managed Security: Изисква ясно определени и прилагани отговорности по отношение на достъпа.

11.7.2. DSS01 – Manage Operations: Включва процедури за управление на логическия достъп и поддържане на сигурна оперативна среда.