					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P04					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**

Съгласуване с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 5.15, 5.17, 5.18	Управление на логическия и физическия достъп
ISO/IEC 27002:2022	Контроли 8.2, 8.3	Контрол на достъпа, базиран на роли, и управление на идентичностите
NIST SP 800-53 Rev.5	AC-1 до AC-20, IA-1 до IA-8	Контроли върху акаунтите и достъпа, идентичността и удостоверяването
GDPR на ЕС	Членове 5(1)(f), 32(1)(b); Съображение 39	Защита на данните и минимизиране на достъпа
NIS2 на ЕС	Член 21(2)(c–e)	Контрол на достъпа, удостоверяване на потребителите и защита на активите
DORA на ЕС	Членове 6, 9(2)	Достъп до ИКТ, потребителски достъп и силни контроли за трети страни
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA	Въвеждане в длъжност, операции, наблюдение и съответствие

1. Цел

1.1 Настоящата политика установява задължителни принципи, отговорности и изисквания за контрол при управлението на достъпа до информационни системи, приложения, физически обекти и информационни активи в цялата организация.

1.2 Тя гарантира, че достъпът се предоставя въз основа на служебна необходимост, длъжностни задължения и рисков профил, като се прилагат принципите за минимално необходим достъп, необходимост да се знае и разделение на отговорностите.

1.3 Политиката подпомага прилагането на клауза 5.15 от ISO/IEC 27001:2022 и свързаните контроли за логически и физически достъп, удостоверяване на потребителите и управление на жизнения цикъл на достъпа.

1.4 Настоящата политика е основополагаща за защитата на цифровите и физическите ресурси от неразрешено използване, злоупотреба или компрометиране.

2. Обхват

2.1 Настоящата политика се прилага за всички потребители, системи и обекти в обхвата на СУИС, включително:

2.1.1 Служители, изпълнители, доставчици и временен персонал

2.1.2 Локална инфраструктура, системи, хоствани в облачна среда, и хибридни среди

2.1.3 Всички корпоративни активи — хардуер, софтуер, данни и защитени физически зони

2.1.4 Логически достъп (напр. системи, мрежи, приложения, API) и физически достъп (напр. сгради, центрове за данни)

2.2 Политиката урежда достъпа през целия жизнен цикъл на идентичността и взаимодействието с ресурсите — от въвеждане в длъжност и предоставяне на достъп до промени в ролята и прекратяване.

2.3 Политиката обхваща също използването на лични устройства за служебни цели (BYOD) и отдалечения достъп, като гарантира, че контролите се прилагат последователно във всички локации и модели на собственост на устройствата.

3. Цели

3.1 Да се прилагат сигурни контроли на достъпа, базирани на роли, които подпомагат оперативната устойчивост и съответствието с регулаторните изисквания.

3.2 Да се гарантира, че правата за достъп се одобряват, наблюдават и отнемат по подходящ начин и своевременно.

3.3 Да се предотвратяват неразрешен достъп, ескалация на привилегии и запазване на неактуални права за достъп.

3.4 Да се подкрепят принципите на Zero Trust, като достъпът по подразбиране се отказва, освен ако не е изрично одобрен и обоснован.

3.5 Да се осигури увереност на одиторите и заинтересованите страни чрез основани на доказателства, автоматизирани прегледи на достъпа и прилагане на политиката.

3.6 Да се интегрира контролът на достъпа в бизнес процесите, събитията от жизнения цикъл по линия на ЧР и техническите архитектури.

4. Роли и отговорности

4.1 Висше ръководство

4.1.1 Одобрява Политиката за контрол на достъпа и осигурява подходящ бюджет и ресурсна обезпеченост за нейното прилагане.

4.1.2 Преглежда рисковете, свързани с контрола на достъпа, в рамките на прегледите от ръководството и разпределя отчетността на стратегическо ниво.

4.2 Директор по информационна сигурност (CISO) / Мениджър на СУИС

4.2.1 Отговаря за рамката за контрол на достъпа и осигурява съответствие с ISO/IEC 27001 и свързаните стандарти.

4.2.2 Координира прилагането на политиката, тестването на контролите и отчитането на метриките за контрол на достъпа.

4.2.3 Осъществява надзор върху моделирането на достъпа въз основа на риска и наблюдава за системни пропуски в контролите.

[... 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 Основания и честота за преглед

9.1.1 Настоящата политика трябва да се преглежда:

9.1.1.1 Ежегодно, или

9.1.1.2 След съществена промяна в ИТ инфраструктурата, регулаторните изисквания или рисковия профил

9.1.1.3 След инциденти, които разкриват слабости в контролите на достъпа

9.1.1.4 При значителни промени в технологиите за удостоверяване или платформите за идентичност

9.2 Отговорност и процес по преглед

9.2.1 CISO или определен ръководител на СУИС управлява цикъла по преглед, като включва:

9.2.1.1 Констатации от вътрешен одит

9.2.1.2 Резултати и метрики от прегледите на достъпа

9.2.1.3 Правни и регулаторни актуализации

9.2.1.4 Промени в технологичните платформи

9.2.2 Всички редакции трябва да бъдат одобрени от висшето ръководство и комуникирани до всички заинтересовани страни.

9.2.3 От засегнатите потребители може да се изиска повторно потвърждение на политиката при съществени актуализации.

9.3 Контрол на версиите и документация

9.3.1 Основната версия се съхранява в Хранилището за документи на СУИС със следните метаданни:

9.3.1.1 Номер на версията и дневник на промените

9.3.1.2 Дата на влизане в сила и дата на следващ преглед

9.3.1.3 Собственик и орган по одобрение

9.3.1.4 Записи за разпространение и потвърждение

9.3.2 Заменените версии трябва да се архивират и да бъдат достъпни за минимален срок от 3 години.

10. Свързани политики и взаимовръзки

10.1 Настоящата политика е функционално свързана със следните документи и трябва да се тълкува заедно с тях:

10.1.1 P01 – Политика за информационна сигурност: Определя ангажимента на организацията към сигурността и очакванията на високо ниво относно контрола на достъпа.

10.1.2 P03 – Политика за приемлива употреба: Установява поведенческите изисквания за достъп и отчетността на потребителите за отговорно използване на системите.

10.1.3 P05 – Политика за управление на промените: Регламентира как промените в конфигурациите за достъп, ролите или груповите структури трябва да се изпълняват и тестват по сигурен начин.

10.1.4 P07 – Политика за въвеждане в длъжност и прекратяване: Регламентира инициирането и отнемането на права за достъп в съответствие със събитията от жизнения цикъл на потребителите.

10.1.5 P11 – Политика за управление на потребителски акаунти и привилегии: Операционализира контролите на ниво акаунт и допълва настоящата политика с насоки за техническо прилагане на контрола на достъпа.

10.2 Заедно тези политики осигуряват единна и приложима рамка за управление на достъпа в различните бизнес звена и технологии.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001:2022:

11.1.1 Клауза 5.15 – Контрол на достъпа: Настоящата политика изпълнява изискването за контрол на достъпа до информация и други свързани активи въз основа на бизнес изискванията и изискванията за информационна сигурност.

11.1.2 Клауза 5.17 – Управление на идентичностите и клауза 5.18 – Информация за удостоверяване: Те се прилагат чрез предоставяне на идентичности, механизми за удостоверяване и присвояване на привилегии.

11.1.3 Контроли от Приложение A 8.2 (Контрол на достъпа) и 8.3 (Управление на идентичностите): Осигуряват основата за целите на контролите в настоящата политика, включително достъп, базиран на роли, интеграция с жизнения цикъл на потребителя и защита на привилегирования достъп.

11.2 NIST SP 800-53 Rev.5:

11.2.1 Семейство AC (AC-1 до AC-20): Настоящата политика подпомага изискванията на NIST за контрол на достъпа както за физически, така и за логически системи, включително дефиниране на политика (AC-1), управление на акаунти (AC-2) и разделение на отговорностите (AC-5).

11.2.2 Семейство IA (IA-1 до IA-8): Предоставя насоки за удостоверяване на идентичността, защита на идентификационните данни и MFA.

11.2.3 AU-2, AU-12: Изискванията за журналиране и одит, прилагани съгласно настоящата политика, подпомагат отчетността на потребителите и разследването на инциденти.

11.2.4 PE-2 до PE-6: Обхващат ограниченията за физически достъп, които настоящата политика частично прилага чрез контрол на пропуски и разрешения за достъп до сгради.

11.3 GDPR на ЕС (2016/679):

11.3.1 Член 5(1)(f): Личните данни трябва да бъдат защитени срещу неразрешен достъп. Настоящата политика осигурява техническото и процедурното прилагане на този принцип.

11.3.2 Член 32(1)(b): Изисква прилагането на контроли на достъпа, псевдонимизация и криптиране за предотвратяване на неразрешено обработване на лични данни.

11.3.3 Съображение 39: Изисква минимизиране на достъпа до лични данни, което тук се прилага чрез минимално необходим достъп и изисквания за обосновка на достъпа.

11.4 Директива NIS2 на ЕС (2022/2555):

11.4.1 Член 21(2)(c–e): Настоящата политика осигурява технически и организационни мерки за контрол на достъпа, удостоверяване на потребителите и защита на активите в съществените и важните субекти.

11.5 DORA на ЕС (2022/2554):

11.5.1 Член 6: Изисква политики за управление на ИКТ риска, които изрично включват управление на потребителския достъп и контроли по жизнения цикъл на идентичността. Настоящата политика изпълнява това изискване за финансовия сектор и сектора на ИКТ услугите.

11.5.2 Член 9(2): Настоящата политика подпомага прилагането на силни контроли на достъпа като част от управлението на ИКТ услуги от трети страни и в рамките на групата.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: Прилага контроли по въвеждане в длъжност и освобождаване в подкрепа на управлението на достъпа.

11.6.2 BAI03 – Managed Solutions Identification and Build: Интегрира изискванията за контрол на достъпа в проектирането на системите и процесите по управление на промените.

11.6.3 DSS01 – Managed Operations и DSS05 – Managed Security Services: Регламентират прилагането на ограниченията за логически достъп и наблюдението за нарушения.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Подпомага механизмите за одит и осигуряване на увереност при валидиране на ефективността на контрола на достъпа.