					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P11					Заглавие на документа: **Политика за управление на потребителски акаунти и привилегии**							
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 6.1.3, Клауза 8	-
ISO/IEC 27002:2022	Контроли 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
GDPR на ЕС	Членове 5(1)(f), 32; Съображение 39	-
NIS2 на ЕС	Членове 21(2)(a, d), 21(3)	-
DORA на ЕС	Членове 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Цел

1 Настоящата политика установява задължителни контроли за управлението на потребителски акаунти и привилегии във всички информационни системи и услуги. Тя гарантира, че достъпът до организационните ресурси се предоставя въз основа на валидирана идентичност, необходимост съгласно ролята и принципите на минималните привилегии и разделението на задълженията.

1.1 Тя подкрепя ангажимента на организацията към информационната сигурност чрез внедряване на структурирани и подлежащи на одит процеси за предоставяне на достъп, присвояване на привилегии, наблюдение на използването и отнемане на акаунти.

1.2 Настоящата политика е от съществено значение за намаляване на риска от неоторизиран достъп, злоупотреба с привилегии, вътрешни заплахи и несъответствие с приложимите регулаторни рамки.

2. Обхват

2.1 Настоящата политика се прилага за всички служители, външни изпълнители, външни доставчици на услуги, консултанти и други лица, на които е предоставен достъп до ИТ ресурсите, приложенията или данните на организацията.

2.2 Тя урежда всички системи и среди, в които се прилагат механизми за автентикация и контрол на достъпа, включително, но не само:

2.2.1 Корпоративни приложения и бази данни

2.2.2 Облачни платформи и SaaS среди

2.2.3 Операционни системи и административни конзоли

2.2.4 Инструменти за отдалечен достъп и VPN

2.2.5 Системи за управление на идентичности и достъп (IAM)

2.3 Политиката обхваща както стандартни, така и привилегировани потребителски акаунти и включва контроли върху:

2.3.1 Създаване, промяна и деактивиране на акаунти

2.3.2 Ескалация и делегиране на привилегии

2.3.3 Контрол и мониторинг на сесии

2.3.4 Методи за автентикация и управление на данните за удостоверяване

3. Цели

3.1 Да се гарантира, че всички потребителски акаунти са еднозначно идентифицируеми, надлежно оторизирани и присвоявани само след формално валидиране на необходимостта.

3.2 Да се прилагат принципите на минималните привилегии и да се предотвратява ненужен или прекомерен достъп чрез налагане на строги контроли върху предоставянето и използването на привилегировани акаунти.

3.3 Да се изисква своевременно актуализиране на статуса на акаунтите при промени в трудовото правоотношение или ролята, включително незабавно деактивиране при прекратяване.

3.4 Да се осигури проактивно откриване и отстраняване на неактивни, неправомерно използвани или неоторизирани акаунти чрез журнали, прегледи и автоматизация.

3.5 Да се поддържа съответствие с ISO/IEC 27001:2022 и свързаните стандарти, както и да се изпълняват задълженията по приложимите правни и регулаторни рамки, като 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 нейното прилагане в цялата организация.

4.1.2 Преглежда и одобрява всички формални изключения или случаи на авариен достъп.

4.1.3 Докладва свързаните с акаунтите одитни констатации и ескалира рисковете към изпълнителното ръководство.

4.2 Мениджър „Контрол на достъпа“ / ИТ администратор

4.2.1 Поддържа и управлява техническите контроли за управление на жизнения цикъл на потребителските акаунти.

4.2.2 Изпълнява действия по предоставяне, отнемане и управление на достъпа и привилегиите след одобрена заявка.

4.2.3 Поддържа официален регистър на всички потребителски акаунти, техния статус и нивото им на привилегии.

4.2.4 Подпомага одити и прегледи по съответствие чрез предоставяне на журнали и отчети за дейността.

[... 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 или при съществени промени в:

9.1.1 Организационната структура или бизнес процесите

9.1.2 ИТ системите, платформите за идентичност или методите за достъп

9.1.3 Регулаторните или договорните изисквания, свързани с управлението на идентичности и достъп

9.2 Директорът по информационна сигурност (CISO), съвместно с Мениджъра „Контрол на достъпа“, отговаря за иницииране на процеса по преглед и координирането на обратната връзка от заинтересованите страни.

9.3 Междинни прегледи могат да бъдат инициирани от:

9.3.1 Инциденти по сигурността, свързани със злоупотреба с акаунти

9.3.2 Одитни констатации, които подчертават дефицити в управлението на жизнения цикъл на акаунтите

9.3.3 Внедряване на нови инструменти за управление на идентичности или привилегирован достъп

9.4 Актуализациите на настоящата политика трябва да бъдат:

9.4.1 Под управление на версиите и регистрирани в библиотеката с документация на СУИС

9.4.2 Комуникирани до всички релевантни заинтересовани страни, включително ръководители на отдели, ИТ операции и ЧР

9.4.3 Подкрепени с актуализирани обучителни материали и процедурни указания

9.5 Всички промени трябва да бъдат одобрени от изпълнителното ръководство или Ръководния комитет по информационна сигурност и журнализирани за целите на одита.

10. Свързани политики и връзки

10.1 Настоящата политика е оперативно свързана и се подпомага от следните свързани политики в рамките на СУИС:

10.1.1 P4 Политика за контрол на достъпа: Установява общите принципи и механизми за контрол на достъпа, включително контроли, базирани на правила и роли.

10.1.2 P7 Политика за назначаване и прекратяване на правоотношения: Определя процедурните стъпки за иницииране и прекратяване на потребителски достъп в съответствие с действията на ЧР.

10.1.3 P8 Политика за осведоменост и обучение по информационна сигурност: Подсилва отговорностите на потребителите относно сигурността на акаунтите и защитата на данните за удостоверяване.

10.1.4 P13 Политика за класификация и етикетиране на данните: Определя нивата на достъп въз основа на класификацията на данните, като гарантира, че границите на привилегиите съответстват на нивата на чувствителност.

10.1.5 P22 Политика за регистриране и мониторинг: Гарантира, че одитна следа се събира за всички дейности, свързани с акаунти, и се преглежда за откриване на аномалии или неоторизирано използване.

10.1.6 P30 Политика за реагиране при инциденти: Регламентира ескалацията, ограничаването и действията след инцидент в случаи на злоупотреба с привилегии или неоторизирана дейност по акаунти.

10.2 Всяка от тези политики действа съвместно с останалите за прилагане на съгласувана, базирана на риска рамка за управление на идентичности и достъп в цялата организация.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с глобално признати стандарти за киберсигурност и регулаторни рамки, които изискват сигурно управление на идентичности, достъп и привилегии като основен компонент на информационната сигурност на организацията.

11.2 ISO/IEC 27001:

11.2.1 Клауза 6.1.3 - изисква организациите да определят, оценяват и третират рисковете за информационната сигурност, което прави управлението на достъпа и привилегиите формален контрол, базиран на риска, вграден в процеса по планиране на СУИС.

11.2.2 Клауза 8.1 - Оперативно планиране и контрол: Подкрепя прилагането на технически и процедурни предпазни мерки, които уреждат потребителския и привилегирования достъп.

11.3 ISO/IEC 27002:2022 - Контроли 5.15 до 5.18:

11.3.1 Контрол 5.15 - Управление на потребителския достъп: Подкрепя формални процеси за предоставяне на достъп, оторизация на достъпа и периодичен преглед на правата за достъп.

11.3.2 Контрол 5.16 - Управление на идентичности: Установява уникалност на идентичността, контроли за жизнения цикъл и прилагане на сигурна автентикация.

11.3.3 Контрол 5.17 - Информация за удостоверяване: Гарантира, че предоставянето и използването на данни за удостоверяване се контролират стриктно, са проследими и са съобразени с принципа на минималните привилегии през целия жизнен цикъл на потребителския акаунт.

11.3.4 Контрол 5.18 - Права за достъп: Адресиран е чрез ролево базирано присвояване на привилегии, одит и изисквания за одобрение на повишен достъп.

11.4 Тези контроли насочват структурираното прилагане на регистрация и дерегистрация на акаунти, разделение на привилегии и използване на информация за удостоверяване. Политиката налага управление на жизнения цикъл на идентичността, достъп точно навреме и мониторинг на сесии с повишени привилегии с цел предотвратяване на неоторизирано използване на системите.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Политика за контрол на достъпа) и AC-2 (Управление на акаунти): Съпоставени чрез изискванията на политиката за одобрения на достъп, съпоставяне на роли и одит на потребителски акаунти.

11.5.2 AC-5 (Разделение на задълженията) и AC-6 (Минимални привилегии): Изпълнени чрез ограничаване на привилегиите, съответствие с длъжностните роли и двойно одобрение за задачи с висок риск.

11.5.3 IA-2 до IA-5 (Идентификация и автентикация): Прилагат се чрез силни механизми за автентикация, правила за жизнения цикъл на данните за удостоверяване и изисквания за MFA.

11.5.4 AU-2, AU-12 (Одитно регистриране и анализ): Адресирани чрез запис на сесии и мониторинг на привилегировани дейности в чувствителни среди.

11.6 GDPR на ЕС (2016/679):

11.6.1 Член 32 - Сигурност на обработването: Изисква контроли за достъп и механизми за проверка на идентичността за защита на личните данни. Изпълнява се чрез задължителни одобрения на акаунти, прегледи на привилегии и силни предпазни мерки за автентикация.

11.6.2 Член 5(1)(f) - Цялостност и поверителност: Гарантира, че личните данни се достъпват само от оторизирани потребители с легитимни роли, подсилено чрез прилагането на управлението на акаунти.

11.6.3 Съображение 39: Изисква ясно ограничаване на достъпа и отчетност — настоящата политика подкрепя пълна проследимост на потребителските идентичности и присвояването на привилегии.

11.7 Директива NIS2 на ЕС (2022/2555):

11.7.1 Член 21(2)(a, d): Изисква организациите да прилагат политики за управление на достъпа и сигурно обработване на данни за удостоверяване и привилегировани сесии, подкрепено чрез контролите в настоящата политика за предоставяне на достъп, мониторинг и изключения.

11.7.2 Член 21(3): Насърчава дисциплина при достъпа и висока степен на увереност в идентичността в критични сектори, постигнати чрез използване на уникални идентификатори, RBAC и ограничен във времето повишен достъп.

11.8 DORA на ЕС (2022/2554):

11.8.1 Член 5 - Управление и контрол на ИКТ: Изисква формализирани процеси за управление на потребителите на ИКТ, покрити чрез документирани процедури за предоставяне на достъп, деактивиране и обработване на изключения.

11.8.2 Член 9 - Управление на риска в ИКТ: Насочва организациите да защитават системите чрез ограничения на достъпа и мониторинг, адресирано чрез MFA, журналиране на привилегирован достъп и централизирани прегледи.

11.9 COBIT 2019:

11.9.1 DSS01 - Управлявани операции: Насърчава прилагането на стандартизирани оперативни контроли, включително управление на жизнения цикъл на потребителските акаунти и документация за достъпа.

11.9.2 DSS05 - Управлявани услуги по сигурност: Отразява сигурното администриране на потребителски и системни привилегии, като подкрепя смекчаването на риска чрез минимални привилегии и валидиране на одитната следа.

11.9.3 APO13 - Управлявана сигурност: Изисква управление на достъпа в рамките на цифровите активи, изпълнено чрез формализирани практики за оторизация на акаунти и роли с изисквания за периодичен преглед.