					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P11S					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	Клаузи 5.3, 8	Роли, отговорности и оперативно планиране/контрол за управление на потребителския достъп
ISO/IEC 27002:2022	Контрол 8	Контроли за предоставяне, преглед и отнемане на повишени привилегии
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Създаване на акаунти, мониторинг, минимални привилегии и разделение на задълженията
EU NIS2	Член 21(2)(d)	Управление на потребителския достъп за съществени и важни субекти
EU DORA	Член 9(2)(b)	Контрол на привилегирован достъп във финансовите субекти
COBIT 2019	DSS05.03, DSS05.04	Предоставяне на достъп, отнемане на достъп и периодичен преглед на потребителския достъп
EU GDPR	Член 32	Подходящи контроли на достъпа за защита на личните данни

1. Цел

1.1 Настоящата политика определя правила за управление на потребителски акаунти и права за достъп по сигурен, последователен и проследим начин. Тя гарантира, че само оправомощени потребители имат достъп до системи и данни и че предоставеният достъп е съобразен с тяхната роля и отговорности.

1.2 Ефективното управление на акаунти и привилегии е от съществено значение за предотвратяване на неоторизиран достъп, ограничаване на вътрешни заплахи и осигуряване на съответствие с ISO/IEC 27001, GDPR и други регулаторни изисквания.

1.3 Настоящата политика позволява на организацията да определи собствеността и отговорността за използването на акаунти, да наблюдава и одитира ескалацията на привилегии и да деактивира или отнема достъп по сигурен начин, когато той вече не е необходим.

1.4 Политиката също така защитава бизнес операциите от оперативни грешки или неправомерна употреба, причинени от прекомерен или ненаблюдаван достъп, и подпомага намаляването на риска от случайно изтичане на данни, неправомерно използване на привилегии или регулаторно несъответствие.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички служители, стажанти, външни изпълнители и потребители от трети страни с достъп до ИТ системите на организацията

2.1.2 Всички системи, устройства, услуги и платформи, управлявани от организацията или от нейно име, включително облачни платформи, локална инфраструктура и инструменти на трети страни

2.2 Политиката обхваща всички видове потребителски акаунти, включително:

2.2.1 Именувани потребителски акаунти (напр. акаунти за електронна поща, системни вписвания)

2.2.2 Администраторски акаунти и акаунти на системно ниво

2.2.3 Временни, гостови или предоставени на трети страни удостоверителни данни за достъп

2.2.4 Служебни акаунти, използвани от приложения или системи за автоматизация

2.3 Политиката се прилага за целия жизнен цикъл на акаунта — от създаване и одобрение до промяна, наблюдение и деактивиране. Това включва първоначално предоставяне на достъп при въвеждане в длъжност, прегледи на достъпа при промяна на ролята и отнемане на достъпа при освобождаване.

3. Цели

3.1 Да се присвояват уникални и проследими потребителски идентичности на всички потребители на системите, като се осигурява отчетност и се елиминира използването на споделени идентификационни данни.

3.2 Да се прилага принципът на минималните привилегии, така че на потребителите да се предоставя само минималното ниво на достъп, необходимо за изпълнение на техните задължения.

3.3 Да се предотвратява неоторизиран достъп до чувствителни системи или данни чрез ясно документирани процеси по одобрение и преглед.

3.4 Да се осигурява своевременно деактивиране на потребителски акаунти, когато те вече не са необходими — напр. при прекратяване, приключване на договор или промяна на ролята.

3.5 Да се поддържа сигурна среда с възможност за доказване на съответствие чрез документиране на всички промени по акаунти, одобрения и периодични прегледи.

3.6 Да се гарантира, че повишаването на привилегии е строго контролирано, независимо одобрявано и журнализирано, а повишеният достъп се отнема своевременно, когато вече не е необходим.

4. Роли и отговорности

4.1 Управител (GM)

4.1.1 Носи цялостна отчетност за прилагането на настоящата политика.

4.1.2 Осигурява практиките за управление на акаунти да са съгласувани с изискванията за сертифициране по ISO/IEC 27001 и приложимите правни задължения (напр. GDPR).

4.1.3 Трябва да бъде незабавно информиран за всеки неоторизиран достъп, инцидент по сигурността или нарушение на политиката, свързани с потребителски акаунти.

4.1.4 Осъществява надзор върху прегледите на политиката, одитите и действията по прилагането ѝ.

4.2 ИТ ръководител или външен доставчик на ИТ услуги

4.2.1 Отговаря за техническото внедряване на контролите за акаунти и привилегии в системите, използвани от организацията.

4.2.2 Предоставя, променя и деактивира потребителски акаунти само въз основа на документирани одобрения.

4.2.3 Прилага изисквания за сложност на паролите, време за автоматично заключване на екрана, многофакторно удостоверяване (когато е налично) и системно журнализиране.

4.2.4 Поддържа защитени записи за всички одобрения за достъп, собственост на акаунти, ескалация на привилегии и отнемане на достъп.

4.2.5 Наблюдава за неоторизирани или осиротели акаунти и докладва несъответствията на GM.

[... 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 от GM и ИТ ръководителя, за да се осигури съответствие със:

9.1.1 Актуалните контроли и насоки на ISO/IEC 27001:2022

9.1.2 Регулаторни промени (напр. GDPR, DORA, NIS2)

9.1.3 Промени в системите, услугите или бизнес структурата

9.2 Прегледи трябва да се извършват и след:

9.2.1 Значими инциденти по сигурността или одитни констатации

9.2.2 Съществени промени в ИТ системите или архитектурата на акаунтите

9.2.3 Въвеждане на нови платформи, изискващи интеграция с контрол на достъпа

9.3 Всички промени трябва да бъдат одобрени от GM и ясно комуникирани на засегнатия персонал.

10. Свързани политики и връзки

10.1 P2S – Политика за роли и отговорности в управлението: Определя отчетността и правомощията за вземане на решения при одобренията за достъп и надзора.

10.2 P4S – Политика за контрол на достъпа: Регламентира прилагането на контрол на достъпа на ниво системи и методи за автентикация.

10.3 P7S – Политика за въвеждане в работата и прекратяване на правоотношенията: Гарантира, че създаването и премахването на акаунти са интегрирани в управляваните от ЧР промени по персонала.

10.4 P8S – Политика за информираност и обучение по информационна сигурност: Обучава потребителите относно сигурни практики при използване на акаунти и очакванията за тяхната употреба.

10.5 P30S – Политика за реагиране при инциденти: Определя действията, които трябва да бъдат предприети, ако неправомерната употреба на акаунт доведе до инцидент по сигурността или неоторизирано разкриване.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 5.3: Изисква ролите и отговорностите по информационната сигурност да бъдат ясно определени и прилагани.

11.1.2 Клауза 8.1: Оперативното планиране и контрол трябва да включват управление на потребителския достъп.

11.2 ISO/IEC 27002

11.2.1 Контрол 8.2: Описва техническите и процедурните контроли за предоставяне, преглед и отнемане на повишени привилегии.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Изисква създаване, мониторинг и отнемане на акаунти въз основа на определени роли и процеси.

11.3.2 AC-5: Разглежда разделението на задълженията с цел предотвратяване на конфликт или злоупотреба с привилегии.

11.3.3 AC-6: Изисква прилагане на принципа на минималните привилегии към всички права за достъп.

11.4 EU GDPR

11.4.1 Член 32: Изисква подходящи контроли на достъпа за защита на личните данни от неоторизиран достъп или промяна.

11.5 EU NIS

11.5.1 Член 21(2)(d): Изисква управление на потребителския достъп като част от основните контроли за сигурност за съществени и важни субекти.

11.6 EU DORA

11.6.1 Член 9(2)(b): Изисква финансовите субекти да прилагат контроли на достъпа, които ограничават и наблюдават привилегированите права.

11.7 COBIT 2019

11.7.1 DSS05.03: Определя предоставянето и отнемането на потребителски достъп като част от управлението на ИТ.

11.7.2 DSS05.04: Изисква текущ преглед и съгласуване на потребителския достъп с организационните роли.