					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P07					Заглавие на документа: **Политика за въвеждане в длъжност и прекратяване на правоотношенията**							
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**

Съгласувана с приложимите стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Clause 7.2, Clause 6	Компетентност на персонала, сигурно интегриране и прилагане на отговорностите при прекратяване/промяна.
ISO/IEC 27002:2022	Controls 6.2, 6.5, 5	Контроли за въвеждане в длъжност, достъп и жизнен цикъл на персонала.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Преход и прекратяване на правоотношения с персонал, принцип на най-малките привилегии, одитно регистриране, управление на достъпа по време и след промени в статуса на персонала.
EU GDPR	Articles 5(1)(f), 25, 32; Recital 39	Ограничаване на достъпа, поверителност, защита и подходящи контроли за данните на персонала.
EU NIS2	Article 21(2)(b, c, d)	Мерки за сигурност на персонала и оперативна сигурност; смекчаване на вътрешни заплахи; процеси по жизнения цикъл.
EU DORA	Articles 5, 8, 9	Управление, вътрешен ИКТ контрол, ИКТ риск, управление на инциденти по време на промени в статуса на персонала.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Човешки ресурси, управление на знанията, сигурност и съответствие при въвеждане в длъжност/прекратяване.

1. Цел

1.1 Настоящата политика установява стандартизирани процедури за управление на въвеждането в длъжност, вътрешните преназначения и прекратяването на правоотношенията за всички видове потребители.

1.2 Тя осигурява своевременно и сигурно предоставяне и отнемане на физически и логически достъп, като същевременно налага изисквания за поверителност, отчетност и връщане на активи.

1.3 Настоящата политика смекчава рисковете, свързани с неоторизиран достъп, изтичане на данни и невърнати активи, чрез интегриране на контролите за въвеждане в длъжност и прекратяване на правоотношенията в процесите на човешки ресурси (ЧР), ИТ и сигурност.

1.4 Тя подпомага изпълнението на ISO/IEC 27001:2022 Annex A Control 6.5, като гарантира, че задълженията по сигурността на персонала се прилагат по време и след трудово или договорно правоотношение.

2. Обхват

2.1 Настоящата политика се прилага за всички служители, външни изпълнители, консултанти, доставчици и други трети страни, на които е предоставен достъп до системите, мрежите, обектите или данните на организацията.

2.2 Тя урежда пълния жизнен цикъл на:

2.2.1 въвеждане в длъжност (наемане, договаряне или временно ангажиране)

2.2.2 вътрешни преназначения или промени в ролята

2.2.3 извеждане (оставка, пенсиониране, прекратяване, изтичане на договор)

2.3 Политиката обхваща:

2.3.1 логически достъп (системи, приложения, облачни услуги, VPN)

2.3.2 физически достъп (пропуски, ключове, системи за контрол на достъпа до сгради)

2.3.3 предоставени активи (лаптопи, телефони, токени, удостоверителни данни)

2.3.4 потвърждение за запознаване с политики и задължения за поверителност

2.4 Всички отдели (ЧР, ИТ, управление на съоръженията и активите, сигурност и ръководство) носят отговорност за изпълнение на своята роля в работните потоци за въвеждане и извеждане.

3. Цели

3.1 Да се гарантира, че на целия персонал се предоставя достъп само след изпълнение на предварителните изисквания за сигурност, обучение и договорни условия.

3.2 Да се отнемат правата за достъп и да се възстановяват организационните активи незабавно при промяна на роля или прекратяване.

3.3 Да се съхранят поверителността, целостта и наличността на организационните активи по време на промени в статуса на персонала.

3.4 Да се подпомогнат одитируемостта и правната защитимост чрез пълни записи за събитията по въвеждане в длъжност и прекратяване.

3.5 Да се намали експозицията към вътрешни заплахи чрез валидиране и документиране на всички събития за достъп, свързани с персонала.

3.6 Да се съгласува жизненият цикъл на персонала в организацията с практики за сигурност, базирани на риска, и регулаторни изисквания.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Одобрява настоящата политика и осигурява правомощия и ресурси за процесите по въвеждане, извеждане и контрол на достъпа.

4.1.2 Гарантира, че промените в статуса на персонала не излагат организацията на неоправдан риск за сигурността или на правен риск.

4.2 Човешки ресурси (ЧР)

4.2.1 Инициира работните потоци за въвеждане и прекратяване за служители и уведомява съответните отдели за промените.

4.2.2 Гарантира, че проверките на миналото, договорите, споразуменията за неразкриване на информация (NDA) и потвържденията за запознаване с политиката са завършени преди предоставяне на достъп.

4.2.3 Информира ИТ и управлението на съоръженията и активите за напускането на служители в съответствие със SLA за уведомяване.

4.2.4 Координира с правни въпроси и съответствие прилагането на задълженията след прекратяване на правоотношението (напр. клаузи за неразкриване).

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Преглед и актуализиране на изискванията

9.1 Честота на преглед на политиката

9.1.1 Настоящата политика трябва да се преглежда:

9.1.1.1 ежегодно, или

9.1.1.2 след всеки съществен инцидент, свързан с неправомерно използване на достъпа, загуба на активи или отказ на процедура

9.1.1.3 при внедряване на съществени промени в платформите на ЧР или IAM

9.1.1.4 при регулаторни или правни промени, засягащи данните на персонала или съответните задължения

9.2 Процес на преглед и собственост

9.2.1 Мениджърът на СУИС и директорът на ЧР координират прегледа с участието на ИТ сигурност, правни въпроси и съответствие.

9.2.2 Всички промени трябва да бъдат одобрени от изпълнителното ръководство и ръководния комитет на СУИС.

9.2.3 Актуализираните версии трябва да бъдат разпространени повторно до засегнатите отдели и персонал за повторно потвърждение.

9.3 Контрол на документа и съхранение

9.3.1 Настоящата политика трябва да включва:

9.3.2 управление на версиите, история на промените и дата на влизане в сила

9.3.3 определен собственик и преглеждащ(и)

9.3.4 класификация на политиката и запис за одобрение

9.3.5 Неактуалните версии се архивират за минимум 3 години в съответствие с Политиката за управление на документи.

10. Свързани политики и връзки

10.1.1 Настоящата политика е пряко интегрирана със:

10.1.2 P1 – Политика за информационна сигурност: Установява целите на организацията по сигурността, включително управлението на достъпа на персонала.

10.1.3 P4 – Политика за контрол на достъпа: Определя оперативните изисквания за предоставяне и отнемане на системен и физически достъп въз основа на тригери за въвеждане и прекратяване.

10.1.4 P3 – Политика за допустима употреба: Изисква потвърждение при въвеждане в длъжност и подпомага прилагането ѝ след прекратяване.

10.1.5 P6 – Политика за управление на риска: Гарантира, че рисковете, свързани с потребителския достъп и промените в статуса, се оценяват и смекчават в съответствие с принципите на СУИС.

10.1.6 P11 – Политика за управление на потребителски акаунти и привилегии: Регламентира техническите контроли за предоставяне и отнемане на достъп в подкрепа на настоящата политика.

10.2 Тези политики формират интегрирана система от контроли за сигурно и отчетно управление на събитията в жизнения цикъл на персонала.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с международно признати рамки за сигурност, поверителност и ИТ управление, за да гарантира, че процесите по въвеждане в длъжност и прекратяване са сигурни, проследими и в съответствие със законовите и организационните изисквания.

11.2 ISO/IEC 27001:

11.2.1 Clause 7.2 – Competence и Clause 6.2 – Information Security Objectives: Настоящата политика подпомага изграждането на компетентност на персонала и сигурното интегриране на лица в роли, които влияят върху целите на СУИС.

11.2.2 Annex A Control 6.5 – Responsibilities After Termination or Change of Employment: Настоящата политика изцяло прилага контроли върху остатъчните права за достъп, съхранението на данни и договорните задължения при напускане.

11.2.3 Annex A Control 5.9 – Screening и 6.2 – Terms and Conditions of Employment: Процедурите по въвеждане в длъжност включват механизми за проверка на миналото и потвърждение за запознаване с политиките в съответствие с тези клаузи.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Personnel Termination) и PS-5 (Personnel Transfer): Настоящата политика налага структурирано премахване или изменение на права за достъп, физически пропуски и активи.

11.3.2 AC-2 (Account Management) и AC-6 (Least Privilege): Разпоредбите гарантират, че достъпът е съобразен с ролята и се отнема своевременно, когато вече не е необходим.

11.3.3 IA-4 (Identifier Management) и IA-5 (Authenticator Management): Подпомага сигурното управление на удостоверителни данни по време и след промени в статуса на персонала.

11.3.4 CM-5 (Access Restrictions for Change): Предотвратява неоторизирани промени след прекратяване чрез отнемане на повишени права за достъп.

11.3.5 AU-2 и AU-6: Журнализирането и проследимостта на събитията по достъпа се подсилват чрез IAM и интеграция с одитната следа.

11.4 EU GDPR (2016/679):

11.4.1 Член 5(1)(f): Защитава личните данни срещу неоторизиран достъп, което тук се прилага чрез отнемане на потребителския достъп при извеждане.

11.4.2 Член 32: Изисква подходящи технически и организационни контроли за защита на личните данни през целия жизнен цикъл на правоотношението.

11.4.3 Член 25 – Защита на данните на етапа на проектиране: Гарантира, че въвеждането в длъжност и прекратяването интегрират минимизиране на данните, съхранение и законосъобразен контрол на достъпа.

11.4.4 Съображение 39: Подчертава ограничаването на достъпа и поверителността, подкрепени от структурата на настоящата политика.

11.5 Директива EU NIS2 (2022/2555):

11.5.1 Член 21(2)(b, c, d): Изисква мерки за сигурност на персонала и оперативна сигурност за адресиране на контрола на достъпа, смекчаването на вътрешни заплахи и процесите по жизнения цикъл, всички от които са отразени в настоящата политика.

11.6 EU DORA (2022/2554):

11.6.1 Член 5 – Управление и вътрешен контрол: Настоящата политика подпомага вътрешното ИКТ управление, свързано с човешкия риск и управлението на достъпа.

11.6.2 Член 8 – Управление на ИКТ риска: Прилага контроли към промените в статуса на персонала, които могат да изложат на риск критични активи или регулирани среди.

11.6.3 Член 9 – Класификация и управление на инциденти: Гарантира, че нарушенията, свързани с прекратяване, подлежат на докладване и се смекчават чрез правилно отнемане на достъп и обработване на активи.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Определя ролите, отговорностите и действията по жизнения цикъл за въвеждане в длъжност и прекратяване, съгласувани с целите на управлението.

11.7.2 BAI08 – Knowledge Management: Подсилва документирането на процедурите, съхраняването на знания и прехвърлянето на контрол в края на правоотношението.

11.7.3 DSS05 – Managed Security Services: Налага деактивиране на потребители, контрол върху активите и отчетност при преходи между роли.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Гарантира, че контролите за въвеждане и извеждане се оценяват по време на вътрешни и външни одити.