					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P07S					Заглавие на документа: **Политика за въвеждане в работа 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**

Съответствие със стандарти и нормативни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 6.2, 7	Изисквания за сигурност в областта на човешките ресурси и осведомеността
ISO/IEC 27002:2022	Контроли 6.2, 6.5	Практики за сигурност при въвеждане в работа и прекратяване на правоотношенията
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Прекратяване на правоотношения на персонал; жизнен цикъл на акаунтите; планиране
EU NIS2	Член 21(2)(h)	Сигурност в областта на човешките ресурси и жизнения цикъл на достъпа
EU DORA	Член 12	Контрол на достъпа и отнемане на достъп до ИКТ системи
COBIT 2019	APO07, DSS01	Сигурност на персонала, контрол на логическия и физическия достъп
EU GDPR	Член 32	Сигурност на личните данни по време на трудовото правоотношение

1. Цел

1.1 Настоящата политика определя процеса по въвеждане в работа на нови служители или външни изпълнители, както и сигурното премахване на достъпа, когато лица напускат или сменят роля.

1.2 Политиката гарантира, че достъпът се предоставя в съответствие с принципа на най-малките привилегии, всички активи се отчитат, а критични действия като деактивиране на системи и възстановяване на данни се изпълняват своевременно.

1.3 Настоящата политика подпомага съответствието, оперативната устойчивост и защитата на данните чрез структурирани и подлежащи на одит дейности по въвеждане и извеждане.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички постоянни и временни служители

2.1.2 Външни изпълнители, консултанти и стажанти

2.1.3 Външни доставчици на услуги със системен или физически достъп

2.2 Тя обхваща:

2.2.1 Въвеждане в работа: създаване на потребителски акаунти, предоставяне на достъп, предоставяне на оборудване

2.2.2 Извеждане: премахване на достъп, връщане на фирмени активи и сигурно закриване на цифрови идентичности

2.2.3 Вътрешни промени в ролите, изискващи преконфигуриране на достъпа или преназначаване на активи

2.3 Политиката се прилага за всички устройства, платформи и местоположения, използвани за изпълнение на служебни функции.

3. Цели

3.1 Да се гарантира, че новоназначеният персонал получава достъп и ресурси въз основа на проверени роли и отговорности.

3.2 Да се потвърди, че достъпът на напускащите потребители е изцяло премахнат от системите и обектите до края на последния им работен ден.

3.3 Да се предотвратят осиротели акаунти и невърнати активи, които създават риск за сигурността.

3.4 Да се поддържат документирани записи за дейностите по въвеждане, преместване и извеждане.

3.5 Да се осигури отчетност чрез контролни списъци и координация между различните функции.

4. Роли и отговорности

4.1 Управител

4.1.1 Одобрява достъпа за привилегировани потребители и упражнява надзор върху процесите по въвеждане и прекратяване.

4.1.2 Гарантира, че изключенията са обосновани и че се предприемат коригиращи действия, когато процесите не се спазват.

4.2 Офис мениджър / Човешки ресурси (ЧР)

4.2.1 Инициира въвеждането в работа на новоназначени лица и уведомява ИТ при напускане.

4.2.2 Осигурява оформянето на необходимите правни документи (напр. споразумение за неразкриване на информация (NDA)) и потвържденията за запознаване с политиките по сигурност.

4.2.3 Поддържа контролни списъци за въвеждане/прекратяване и следи за спазването на политиката.

[... 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

9.1.1 Настоящата политика трябва да се преглежда най-малко веднъж годишно от Управителя и ръководителите на ЧР/ИТ.

9.2 Основания за извънреден преглед

9.2.1 Актуализации трябва да се извършват, ако:

9.2.1.1 Бъдат въведени нови системи за ЧР или ИТ

9.2.1.2 Има промяна на външния доставчик на ИТ услуги или на доставчика на управлявани ЧР услуги

9.2.1.3 Одити по сигурността установят пропуски в процеса

9.2.1.4 Правните задължения се променят (напр. актуализации по GDPR)

9.2.1.5 Възникне критичен неуспех при извеждане или нарушение на сигурността

9.3 Управление на версиите и одобрение

9.3.1 Всяка версия на настоящата политика трябва да включва:

9.3.1.1 Номер на версия и дата

9.3.1.2 Обобщение на промените

9.3.1.3 Одобрение от Управителя

9.3.1.4 Архивирани предходни версии, съхранявани най-малко три години

9.4 Комуникация и потвърждение

9.4.1 Всички служители, които отговарят за въвеждане или прекратяване, трябва да бъдат уведомени за всички актуализации на политиката. Ежегодните инструктажи за осведоменост или опреснителните инструктажи са задължителни.

10. Свързани политики и връзки

10.1 Настоящата политика подкрепя и се подкрепя от следните документи:

10.1.1 P2S – Политика за роли и отговорности в управлението: Осигурява отчетност в процесите по достъп и въвеждане

10.1.2 P4S – Политика за контрол на достъпа: Установява техническото прилагане на предоставянето на достъп въз основа на роли и деактивирането

10.1.3 P6S – Политика за управление на риска: Оценява рисковете, произтичащи от откази на контролите при въвеждане и прекратяване

10.1.4 P8S – Политика за осведоменост и обучение по информационна сигурност: Установява изискванията за инструктаж на персонала при въвеждане

10.1.5 P30S – Политика за реагиране при инциденти: Третира неуспеха при отнемане на достъп или кражбата на активи като инциденти по сигурността

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 6.2 – Установява изисквания за сигурност в областта на човешките ресурси

11.1.2 Клауза 7.2 – Въвежда задължение за обучение за осведоменост на новия персонал

11.2 ISO/IEC 27002

11.2.1 Контроли 6.2 и 6.5 – Описват практики за сигурност при въвеждане в работа и прекратяване на правоотношенията

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Процедури за прекратяване на правоотношения на персонал, включително деактивиране на достъпа

11.3.2 AC-2 – Осигурява управление на жизнения цикъл на акаунтите за потребителски достъп

11.3.3 PL-4 – Изисква планиране на преходите на персонала

11.4 EU GDPR

11.4.1 Член 32 – Осигурява подходящо ниво на сигурност по време и след трудовото правоотношение, особено по отношение на достъпа до лични данни

11.5 Директива NIS2 на ЕС

11.5.1 Член 21(2)(h) – Изисква контроли за сигурност в областта на човешките ресурси и жизнения цикъл на достъпа

11.6 EU DORA

11.6.1 Член 12 – Изисква регулираните финансови субекти да контролират достъпа на персонала до ИКТ системи, включително процедури за отнемане на достъп

11.7 COBIT 2019

11.7.1 APO07 – Управление на човешките ресурси: Установява изисквания за сигурност по жизнения цикъл на персонала

11.7.2 DSS01 – Управление на операциите: Обхваща контрола на логическия и физическия достъп при преходи в трудовото правоотношение