					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P10S					Заглавие на документа: **Политика за чисто бюро и заключен екран**							
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 със стандарти и регулации

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клаузи 7.2, 8	
ISO/IEC 27002:2022	Контрол 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Директива ЕС NIS2	Член 21(2)(d)	
Регламент ЕС DORA	Член 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
Регламент (ЕС) 2016/679 (GDPR)	Член 32	

1. Цел

1.1 Настоящата политика установява задължителни правила за поддържане на сигурна работна среда, като гарантира, че бюрата, работните станции и екраните не остават с видима поверителна информация, когато са без надзор.

1.2 Основната ѝ цел е да предотвратява неоторизиран достъп до чувствителна информация чрез оставени без надзор разпечатки, отключени екрани или неправилно съхранявани преносими носители както в офис среда, така и при дистанционна работа.

1.3 Практиките за чисто бюро и заключен екран, определени в тази политика, укрепват способността на организацията да изпълнява изискванията за сертифициране по ISO/IEC 27001 чрез свеждане до минимум на предотвратимите рискове от разкриване на информация. Тези практики също така дават увереност на клиенти, партньори и одитори, че организацията приема информационната сигурност сериозно, включително в среди с ограничени ресурси.

1.4 Настоящата политика подкрепя култура на отчетност и осведоменост, като гарантира, че целият персонал — независимо от ролята или техническата експертиза — разбира своята отговорност да защитава информацията на дружеството и клиентите от визуално разкриване, кражба или загуба.

2. Обхват

2.1 Настоящата политика се прилага за:

2.1.1 Всички служители, външни изпълнители, стажанти и временни работници, които използват притежавани от дружеството или лично предоставени работни станции, бюра или мобилни устройства

2.1.2 Всички физически локации, използвани за служебна дейност, включително самостоятелни офиси, споделени работни пространства и дистанционни/домашни работни места

2.1.3 Всички цифрови устройства с възможност за визуализация, включително настолни компютри, лаптопи, таблети и външни монитори, използвани за служебни цели

2.2 Политиката обхваща всеки физически или цифров актив, който може да визуализира, съдържа или предава чувствителна информация, включително:

2.2.1 Печатни записи или ръкописни бележки

2.2.2 USB устройства, CD дискове и външни твърди дискове

2.2.3 Мобилни телефони, използвани за служебни съобщения или електронна поща

2.2.4 Компютърни монитори и проектори, свързани към работни системи

2.3 Настоящата политика остава приложима извън редовното работно време и при нестандартни дейности (напр. поддръжка извън работно време или работа по реагиране при инциденти).

3. Цели

3.1 Да се прилагат практически и последователни контроли, които гарантират, че на бюра, екрани или в общи пространства не остава открита чувствителна информация.

3.2 Да се сведе до минимум рискът от неоторизиран достъп както от вътрешни източници (напр. непреднамерен достъп от други служители), така и от външни заплахи (напр. посетители, почистващ персонал или външни изпълнители).

3.3 Да се подпомогнат ограниченията за физически и логически достъп, като от персонала се изисква активно да защитава работните материали и да заключва компютрите си, когато са без надзор.

3.4 Да се повиши осведомеността на персонала относно сигурните работни практики и да се въведат ясни, задължителни правила, приложими в ежедневната работа независимо от местоположението, от което се работи.

3.5 Да се осигури съответствие с Приложение A, контрол 7.7 на ISO/IEC 27001 и насоките за прилагането му по ISO/IEC 27002 относно изискванията за чисто бюро и заключен екран.

3.6 Да се гарантира, че организацията може да демонстрира дължима грижа и готовност за одит, без да е необходима инфраструктура от корпоративен клас.

4. Роли и отговорности

4.1 Управител

4.1.1 Отговаря за тази политика и гарантира, че тя е надлежно комуникирана, разбрана и спазвана от всички служители и външни изпълнители.

4.1.2 Отговаря за одобряването на всички изключения, реагирането при нарушения и надзора върху обученията, свързани със сигурни работни практики.

4.1.3 Трябва да извършва или да възлага редовни проверки (най-малко веднъж на тримесечие), за да потвърди, че физическите и цифровите работни пространства отговарят на изискванията на политиката.

4.2 Определен служител (ако е приложимо)

4.2.1 На него може да бъде възложена отговорност за внедряване на технически конфигурации (напр. настройки за изтичане на времето до заключване на екрана) или за осигуряване на средства за физическо съхранение (напр. заключващи се чекмеджета).

4.2.2 Подпомага Управителя, като докладва случаи на несъответствие, напомня за изискванията за сигурност на работното място и проследява действията за отстраняване, когато бъдат установени проблеми.

4.2.3 Съдейства за осигуряване на подходящи механизми за заключване или защитени пространства за съхранение за всички служители, когато това е практически възможно.

[... 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 Управителят трябва да преглежда тази политика най-малко веднъж годишно и след настъпване на някое от следните събития:

9.1.1 Въвеждане на нови офис пространства, устройства или споделени системи

9.1.2 Промени в приложимите правни изисквания или изискванията за сертифициране

9.1.3 Констатации от одити, оценки на риска или инциденти по сигурността

9.2 Междинните актуализации трябва да бъдат съобщавани на всички служители по електронна поща, като се изисква потвърждение за запознаване.

9.3 Предходните версии на тази политика трябва да се съхраняват сигурно и да подлежат на одит, за да доказват текущо съответствие с ISO/IEC 27001 и свързаните рамки.

10. Свързани политики и връзки

10.1 P2S – Политика за роли и отговорности в управлението: Уточнява правомощията на Управителя да прилага политиката и да извършва одит на поведението във физическите и цифровите работни пространства.

10.2 P4S – Политика за контрол на достъпа: Подкрепя техническото прилагане на заключването на екрана и практиките за сигурно влизане в работни станции.

10.3 P8S – Политика за информираност и обучение по информационна сигурност: Подсилва поведенческото обучение, необходимо за съответствие с политиката.

10.4 P17S – Политика за защита на данните и поверителност: Определя задълженията за боравене и защита на лични данни и чувствителни данни в съответствие с GDPR.

10.5 P30S – Политика за реагиране при инциденти: Осигурява рамката за ескалация и реагиране, ако нарушение доведе до разкриване на данни или инцидент по сигурността.

11. Референтни стандарти и рамки

11.1 ISO/IEC 27001

11.1.1 Клауза 7.2: Изисква целият персонал да е запознат със своите отговорности по сигурността, включително физическите предпазни мерки.

11.1.2 Клауза 8.1: Оперативните контроли трябва да осигуряват подходящи физически и логически защити.

11.2 ISO/IEC 27002

11.2.1 Контрол 7.7: Предоставя подробни насоки за установяване, комуникиране и прилагане на изисквания за чисто бюро и заключен екран.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Установява очаквания за контрол на физическия достъп, включително поведението на персонала в защитена среда.

11.3.2 AC-11: Изисква функционалност за заключване на сесията на работните станции с цел предотвратяване на неоторизирано преглеждане или взаимодействие.

11.4 GDPR

11.4.1 Член 32: Изисква организациите да защитават личните данни чрез физически и технически предпазни мерки, включително по отношение на работни станции и документи.

11.5 Директива ЕС NIS2

11.5.1 Член 21(2)(d): Изисква организациите да прилагат политики за физически и логически достъп, базирани на риска.

11.6 Регламент ЕС DORA

11.6.1 Член 9(2)(f): Изисква политики за сигурност на ИКТ, включително сигурна хигиена на работното пространство, за организациите от финансовия сектор и техните вериги на доставки.

11.7 COBIT 2019

11.7.1 DSS01.06: Изисква практики за защита на активите, включително физически контроли върху работните пространства и носителите.

11.7.2 DSS05.02: Подкрепя прилагането на практики за сигурност на крайните потребители в различни оперативни среди.