					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: P10					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**

Съответствие със стандарти и регулаторни изисквания

Стандарт/регулация	Клауза/член	Коментар
ISO/IEC 27001:2022	Клауза 6.1.3, Клауза 8	План за третиране на риска, оперативно планиране и контрол за сигурни работни пространства
ISO/IEC 27002:2022	Контрол 7	Поведенчески и средови контроли за защита на физическа информация, оставена без надзор
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Физически достъп, сигурност на външния персонал, унищожаване на носители, заключване на сесии, контрол на конфигурацията и управление на удостоверителните данни
EU GDPR	Членове 5(1)(f), 32; Съображение 39	Цялост на данните, поверителност и физически мерки за защита на данните
EU NIS2	Членове 21(2)(d), 21(3)	Политики за физическа сигурност, поведение на потребителите и предотвратяване на изтичане на информация
EU DORA	Членове 5, 8, 9	Вътрешно управление, управление на ИКТ риска и инциденти, включително аспекти на физическата сигурност
COBIT 2019	DSS01, DSS05, MEA	Управлявани операции, управлявани услуги по сигурността и мониторинг на съответствието

1. Цел

1.1 Настоящата политика установява задължителни контроли за защита на чувствителна информация, като изисква сигурно боравене с физически документи, работни станции, екрани и преносими носители както в офисна среда, така и в споделени работни пространства.

1.2 Тя подпомага Контрол 7.7 от Приложение A на ISO/IEC 27001 чрез прилагане на поведенчески и технически практики, които намаляват риска от неоторизирано разкриване, кражба или загуба на данни поради информация, оставена без надзор или видима за неупълномощени лица.

1.3 Настоящата политика укрепва физическата и информационната сигурност в ежедневните операции и подпомага съответствието с приложимите правни, договорни и регулаторни задължения.

2. Обхват

2.1 Настоящата политика се прилага за целия персонал, който работи във физически работни пространства или има достъп до тях, включително:

2.1.1 Постоянни и временни служители

2.1.2 Външни изпълнители, консултанти, доставчици и стажанти

2.1.3 Външни доставчици на услуги и посетители на място с достъп до чувствителна информация

2.2 Изискванията се прилагат в:

2.2.1 Индивидуални офиси, работни клетки и работни пространства с отворен план

2.2.2 Заседателни зали и споделени зони за сътрудничество

2.2.3 Зони с принтери, рецепции и помещения за копиране

2.2.4 Зони, в които се използват отдалечени работни станции или споделени терминали

2.3 Настоящата политика се прилага и за временни или хибридни работни среди (напр. споделени работни места), както и за публично достъпни среди, в които съществува риск от наблюдение през рамо или наличие на данни, оставени без надзор.

3. Цели

3.1 Да се предотврати неоторизиран достъп до поверителна, чувствителна или регулирана информация, оставена незащитена във физическа или цифрова форма.

3.2 Да се осигури стандартизирано ниво на сигурност във всички работни среди чрез използване на физически предпазни мерки, конфигурация на работните станции и поведение на крайните потребители.

3.3 Да се намали рискът от нарушения на поверителността, загуба на интелектуална собственост и изтичане на данни, причинени от небрежност или пропуск.

3.4 Да се утвърди поведение за чисто бюро и заключен екран като част от организационната култура в подкрепа на оперативната дисциплина, възможността за одит и правната защитимост.

3.5 Да се подпомогне съответствието с ISO/IEC 27001, член 32 от GDPR, член 15 от NIS2 и други изисквания за физическа сигурност, приложими към критични или лични данни.

4. Роли и отговорности

4.1 Изпълнително ръководство

4.1.1 Утвърждава настоящата политика и насърчава култура на осведоменост по сигурността във всички бизнес звена.

4.1.2 Осигурява подходящи ресурси за прилагане на политиката, кампании за осведоменост и механизми за физически контрол.

4.2 Директор по информационна сигурност (CISO) / Мениджър на СУИС

4.2.1 Отговаря за настоящата политика и осигурява съгласуваността ѝ с ISO/IEC 27001:2022, изискванията за одит и стратегиите за третиране на риска.

4.2.2 Разработва програми за осведоменост и контроли, за да осигури последователно прилагане във всички обекти и хибридни работни среди.

4.2.3 Координира действията с екипите по управление на сградния фонд и ИТ, за да гарантира наличието на подходящи физически предпазни мерки.

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

9. Преглед и актуализация на изискванията

9.1 График за преглед на политиката

9.1.1 Настоящата политика трябва да се преглежда:

9.1.1.1 Най-малко веднъж годишно

9.1.1.2 След всяко одитно несъответствие, свързано с работно пространство или видимост на екрани

9.1.1.3 След физически или средов инцидент (напр. кражба на устройство, неразрешено следване при влизане, наблюдение)

9.1.1.4 При внедряване на нови офисни разпределения, политики за управление на сградния фонд или модели на работно пространство (напр. hot-desking, отдалечени хъбове)

9.2 Отговорни собственици

9.2.1 Собственик на политиката е директорът по информационна сигурност (CISO) или назначеният Мениджър на СУИС.

9.2.2 Процесът по преглед трябва да включва:

9.2.2.1 Екипите по управление на сградния фонд и корпоративна сигурност

9.2.2.2 ИТ и инфраструктура за прилагане на контролите, свързани с устройствата

9.2.2.3 Човешки ресурси (ЧР) и Правен отдел за прилагане на поведенческите изисквания и съгласуване на дисциплинарните мерки

9.2.3 Всички актуализации на политиката трябва да бъдат под управление на версиите, одобрени от Ръководния комитет на СУИС и разпространени повторно с ново потвърждение, когато това се изисква.

9.3 Комуникация при промени

9.3.1 Потребителите трябва да бъдат уведомявани за съществени актуализации чрез:

9.3.1.1 Център за политики в интранет или портал

9.3.1.2 Целенасочени имейл съобщения

9.3.1.3 Опреснителни обучения при въвеждане в длъжност и тримесечни инструктажи

9.3.1.4 Задължителни подкани за потвърждение при нови критични клаузи по прилагането

10. Свързани политики и връзки

10.1 Настоящата политика е съгласувана със следните документи и ги подпомага:

10.1.1 P1 – Политика за информационна сигурност: Определя очакванията за поведение на потребителите и физическа сигурност, които са в основата на настоящата политика.

10.1.2 P3 – Политика за допустима употреба: Разглежда отчетността на потребителите за защитата на данни и системи, включително във физическа среда.

10.1.3 P6 – Политика за управление на риска: Включва рисковете, свързани с физическите работни пространства, като част от анализа на информационния риск в цялата организация.

10.1.4 P12 – Политика за управление на активите: Подпомага проследяването и сигурното боравене с устройства и носители, оставени върху бюра.

10.1.5 P13 – Политика за класификация и етикетиране на данните: Свързва прилагането на изискванията за чисто бюро с физически документи, обозначени като „Поверително“ или „За вътрешна употреба“.

10.1.6 P14 – Политика за съхранение и унищожаване на данни: Регламентира срока за съхранение на физически документи, шредиране и практики за работа с контейнери за унищожаване.

10.1.7 P22 – Политика за регистриране и мониторинг: Може да се използва за наблюдение на статуса на заключване на работните станции, времето на неактивност или видеонаблюдение на работни пространства, когато това е разрешено.

10.2 Тези свързани политики формират интегрирана култура на сигурност, съчетаваща осведоменост на потребителите, физически предпазни мерки и отчетност за осигуряване на устойчиви работни пространства.

11. Референтни стандарти и рамки

11.1 Настоящата политика е съгласувана с глобално признати стандарти и правни изисквания, които налагат защита на чувствителната информация във физическа среда и чрез поведението на потребителите.

11.2 ISO/IEC 27001

11.2.1 Клауза 6.1.3 – План за третиране на риска: Подпомага внедряването на контроли за смекчаване на физически и средови рискове, включително такива, свързани с поведението на потребителите в отворени работни пространства.

11.2.2 Клауза 8.1 – Оперативно планиране и контрол: Установява оперативни предпазни мерки за управление на сигурни работни пространства и използване на оборудване.

11.3 ISO/IEC 27002:2022 – Контрол 7

11.3.1 Този контрол изисква поведенчески и средови мерки за защита с цел предотвратяване на неоторизиран достъп до информация чрез носители, екрани или отпечатани материали, оставени без надзор. Политиката налага добра практика за физическите работни пространства, използване на заключен екран и унищожаване на чувствителни документи.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Разрешения за физически достъп): Свързан е с ограниченията за работните пространства и прилагането на заключено съхранение в среди с висок риск.

11.4.2 PS-7 (Сигурност на външния персонал): Прилага се чрез изискванията за чисто бюро и заключен екран, разширени към външни изпълнители и потребители от трети страни.

11.4.3 MP-6 (Саниране на носители) и AC-11 (Заключване на сесия): Реализират се чрез процедури за сигурно унищожаване и задължителни таймери за заключване на екрана.

11.4.4 CM-6 (Настройки на конфигурацията) и IA-5 (Управление на удостоверителите): Подпомагат техническото прилагане на заключване на екрана и контрол на сесиите върху крайните устройства.

11.5 EU GDPR (2016/679)

11.5.1 Член 5(1)(f): Налага цялост и поверителност на личните данни, включително защита срещу физическо излагане или преглед от неупълномощени лица.

11.5.2 Член 32 – Сигурност на обработването: Изисква подходящи физически и организационни мерки за защита на личните данни от случайно или неправомерно унищожаване, загуба или неоторизирано разкриване — постигнато чрез контролите за бюро и екран.

11.5.3 Съображение 39: Изисква ограничаване на достъпа до лични данни само до упълномощени лица — това включва и защитата им във физическа форма, когато са оставени без надзор.

11.6 Директива NIS2 на ЕС (2022/2555)

11.6.1 Член 21(2)(d): Изисква политики и процедури, свързани с физическата сигурност и сигурността на средата, включително защита на информацията на ниво работно място.

11.6.2 Член 21(3): Насърчава култура на сигурност, която включва добро поведение на потребителите, осведоменост и предотвратяване на неволно изтичане на данни — подкрепено от поведенческите контроли в настоящата политика.

11.7 EU DORA (2022/2554)

11.7.1 Член 5 – Вътрешно управление и контрол: Изисква всички рискове, свързани с ИКТ, включително човешки и средови заплахи, да бъдат управлявани чрез приложими политики.

11.7.2 Член 8 – Управление на ИКТ риска: Изисква предпазни мерки както в цифров, така и във физически контекст, като гарантира, че потребителите, работещи от разстояние, в клонове или в локална среда, не създават неуправлявана експозиция.

11.7.3 Член 9 – Управление на инциденти: Изисква средови или поведенчески пропуски, водещи до експозиция на данни, да бъдат регистрирани, класифицирани и обработвани с подходящи коригиращи действия.

11.8 COBIT 2019

11.8.1 DSS01 – Управлявани операции: Осигурява оперативна дисциплина при защита на физически работни пространства и системи чрез повтаряеми контроли.

11.8.2 DSS05 – Управлявани услуги по сигурността: Подпомага защитата на данни, устройства и крайни точки за достъп чрез поведенчески механизми за прилагане, като практиките за чисто бюро.

11.8.3 MEA03 – Мониторинг, оценяване и преценка на съответствието: Насърчава одитирането на физически предпазни мерки и възприемането на политиката в ежедневните бизнес практики.