					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P10S					Tytuł dokumentu: **Polityka czystego biurka i ekranu**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 7.2, 8	
ISO/IEC 27002:2022	Środek kontrolny 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Dyrektywa NIS2	Artykuł 21(2)(d)	
Rozporządzenie DORA	Artykuł 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
RODO	Artykuł 32	

1. Cel

1.1 Niniejsza polityka ustanawia obowiązujące zasady utrzymania bezpiecznego środowiska pracy poprzez zapewnienie, że biurka, stacje robocze i ekrany nie zawierają widocznych informacji poufnych, gdy pozostają bez nadzoru.

1.2 Jej głównym celem jest zapobieganie nieuprawnionemu dostępowi do informacji wrażliwych wskutek pozostawionych bez nadzoru wydruków, niezablokowanych ekranów lub niewłaściwie przechowywanych nośników wymiennych, zarówno w fizycznych środowiskach biurowych, jak i w lokalizacjach pracy zdalnej.

1.3 Praktyki czystego biurka i ekranu określone w niniejszej polityce wzmacniają zdolność organizacji do spełnienia wymagań certyfikacyjnych ISO/IEC 27001 poprzez ograniczenie możliwych do uniknięcia ryzyk ujawnienia informacji. Praktyki te potwierdzają również klientom, partnerom i audytorom, że organizacja poważnie traktuje bezpieczeństwo informacji, także w środowiskach o ograniczonych zasobach.

1.4 Niniejsza polityka wspiera kulturę rozliczalności i świadomości, zapewniając, że cały personel — niezależnie od roli lub poziomu wiedzy technicznej — rozumie swoją odpowiedzialność za ochronę informacji organizacji i klientów przed ujawnieniem poprzez wgląd, kradzieżą lub utratą.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników, kontraktorów, stażystów i personelu tymczasowego korzystających ze stacji roboczych, biurek lub urządzeń mobilnych będących własnością organizacji lub przydzielonych im do użytku służbowego,

2.1.2 wszystkich lokalizacji fizycznych wykorzystywanych do prowadzenia działalności, w tym wydzielonych biur, przestrzeni coworkingowych oraz zdalnych/domowych miejsc pracy,

2.1.3 wszystkich urządzeń cyfrowych wyposażonych w funkcje wyświetlania, w tym komputerów stacjonarnych, laptopów, tabletów oraz monitorów zewnętrznych wykorzystywanych do celów służbowych.

2.2 Polityka obejmuje każdy składnik fizyczny lub cyfrowy, który może wyświetlać, zawierać lub przekazywać informacje wrażliwe, w tym:

2.2.1 wydruki oraz odręczne notatki,

2.2.2 nośniki USB, płyty CD oraz zewnętrzne dyski twarde,

2.2.3 telefony komórkowe wykorzystywane do komunikacji służbowej lub obsługi poczty elektronicznej,

2.2.4 monitory komputerowe i projektory podłączone do systemów roboczych.

2.3 Niniejsza polityka obowiązuje również poza standardowymi godzinami pracy oraz podczas działań niestandardowych (np. prac serwisowych po godzinach lub działań podejmowanych w odpowiedzi na sytuacje awaryjne).

3. Cele

3.1 Wdrożenie praktycznych i spójnych mechanizmów kontrolnych zapewniających, że żadne informacje wrażliwe nie pozostają ujawnione na biurkach, ekranach ani we wspólnych przestrzeniach.

3.2 Ograniczenie ryzyka nieuprawnionego dostępu, zarówno ze źródeł wewnętrznych (np. niezamierzonego dostępu przez innych pracowników), jak i zagrożeń zewnętrznych (np. ze strony gości, personelu sprzątającego lub kontraktorów).

3.3 Wspieranie ograniczeń dostępu fizycznego i logicznego poprzez wymaganie od personelu aktywnego zabezpieczania materiałów roboczych i blokowania komputerów na czas nieobecności.

3.4 Budowanie świadomości personelu w zakresie bezpiecznych praktyk pracy oraz zapewnienie prostych, egzekwowalnych zasad mających zastosowanie w codziennej działalności, niezależnie od miejsca wykonywania pracy.

3.5 Zapewnienie zgodności z załącznikiem A do ISO/IEC 27001, środkiem kontrolnym 7.7, oraz z wytycznymi wdrożeniowymi zawartymi w ISO/IEC 27002 dotyczącymi wymagań w zakresie czystego biurka i ekranu.

3.6 Zapewnienie, że organizacja może wykazać należytą staranność oraz gotowość do audytu bez konieczności posiadania infrastruktury klasy korporacyjnej.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Jest właścicielem niniejszej polityki i zapewnia jej właściwe zakomunikowanie, zrozumienie oraz przestrzeganie przez wszystkich pracowników i kontraktorów.

4.1.2 Odpowiada za zatwierdzanie wszelkich odstępstw, reagowanie na naruszenia oraz nadzór nad szkoleniami dotyczącymi bezpiecznych praktyk pracy.

4.1.3 Musi przeprowadzać lub delegować regularne kontrole (co najmniej raz na kwartał) w celu potwierdzenia, że fizyczne i cyfrowe przestrzenie pracy spełniają wymagania niniejszej polityki.

4.2 Wyznaczony członek personelu (jeżeli został wyznaczony)

4.2.1 Może otrzymać odpowiedzialność za wdrożenie konfiguracji technicznych (np. ustawień limitu czasu ekranu) lub dystrybucję fizycznych rozwiązań do przechowywania (np. zamykanych szuflad).

4.2.2 Wspiera GM poprzez zgłaszanie niezgodności, przekazywanie przypomnień dotyczących bezpieczeństwa miejsca pracy oraz monitorowanie działań naprawczych po zidentyfikowaniu problemów.

4.2.3 Pomaga zapewnić, aby wszyscy pracownicy mieli dostęp do odpowiednich mechanizmów zamykania lub bezpiecznych miejsc przechowywania, tam gdzie jest to wykonalne.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 GM musi dokonywać przeglądu niniejszej polityki co najmniej raz w roku oraz po wystąpieniu któregokolwiek z poniższych zdarzeń:

9.1.1 wprowadzenia nowych przestrzeni biurowych, urządzeń lub systemów współdzielonych,

9.1.2 zmian w mających zastosowanie wymaganiach prawnych lub certyfikacyjnych,

9.1.3 ustaleń wynikających z audytów, ocen ryzyka lub incydentów bezpieczeństwa.

9.2 Aktualizacje międzyokresowe muszą być komunikowane wszystkim pracownikom pocztą elektroniczną, z wymaganym potwierdzeniem zapoznania się.

9.3 Poprzednie wersje niniejszej polityki muszą być bezpiecznie przechowywane i możliwe do prześledzenia na potrzeby audytu w celu wykazania ciągłej zgodności z ISO/IEC 27001 i powiązanymi ramami.

10. Powiązane polityki i zależności

10.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: wyjaśnia uprawnienia GM do egzekwowania polityki i prowadzenia audytów zachowań w fizycznych i cyfrowych przestrzeniach pracy.

10.2 P4S – Polityka kontroli dostępu: wspiera techniczne wdrożenie blokady ekranu i bezpiecznych praktyk logowania do stacji roboczych.

10.3 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: wzmacnia szkolenia behawioralne niezbędne do zapewnienia zgodności z polityką.

10.4 P17S – Polityka ochrony danych i prywatności: określa obowiązki dotyczące postępowania z danymi osobowymi i informacjami wrażliwymi oraz ich zabezpieczania zgodnie z RODO.

10.5 P30S – Polityka reagowania na incydenty: zapewnia ramy eskalacji i reagowania, jeżeli naruszenie skutkuje ujawnieniem danych lub incydentem bezpieczeństwa.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 7.2: wymaga, aby cały personel był świadomy obowiązków w zakresie bezpieczeństwa, w tym zabezpieczeń fizycznych.

11.1.2 Klauzula 8.1: środki kontroli operacyjnej muszą zapewniać odpowiednie zabezpieczenia fizyczne i logiczne.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 7.7: zawiera szczegółowe wytyczne dotyczące ustanawiania, komunikowania i stosowania wymagań w zakresie czystego biurka i ekranu.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: określa oczekiwania w zakresie kontroli dostępu fizycznego, w tym zachowania personelu w bezpiecznych środowiskach.

11.3.2 AC-11: wymaga funkcji blokady sesji dla stacji roboczych w celu zapobiegania nieuprawnionemu wglądowi lub interakcji.

11.4 RODO

11.4.1 Artykuł 32: wymaga, aby organizacje chroniły dane osobowe przy użyciu zabezpieczeń fizycznych i technicznych, w tym w odniesieniu do stacji roboczych i dokumentów.

11.5 Dyrektywa NIS2

11.5.1 Artykuł 21(2)(d): wymaga, aby organizacje wdrożyły oparte na ryzyku polityki dostępu fizycznego i logicznego.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 9(2)(f): wymaga polityk bezpieczeństwa ICT, w tym bezpiecznej higieny przestrzeni roboczej, dla podmiotów sektora finansowego i ich łańcuchów dostaw.

11.7 COBIT 2019

11.7.1 DSS01.06: wymaga praktyk ochrony aktywów, w tym mechanizmów kontroli fizycznej dotyczących przestrzeni roboczych i nośników.

11.7.2 DSS05.02: wspiera stosowanie praktyk bezpieczeństwa użytkowników końcowych w różnych środowiskach operacyjnych.