					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P10					Tytuł dokumentu: **Polityka czystego biurka i czystego 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	Klauzula 6.1.3, Klauzula 8	plan postępowania z ryzykiem, planowanie operacyjne i nadzór nad bezpiecznymi przestrzeniami roboczymi
ISO/IEC 27002:2022	Środek kontrolny 7	zabezpieczenia behawioralne i kontrole środowiskowe służące ochronie informacji fizycznych pozostawionych bez nadzoru
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	dostęp fizyczny, bezpieczeństwo personelu zewnętrznego, utylizacja nośników, blokada sesji, konfiguracja oraz kontrole mechanizmów uwierzytelniania
RODO	Artykuły 5(1)(f), 32; Motyw 39	integralność danych, poufność oraz fizyczne środki ochrony danych
Dyrektywa NIS2	Artykuły 21(2)(d), 21(3)	polityki dotyczące bezpieczeństwa fizycznego, zachowań użytkowników i zapobiegania wyciekom danych
Rozporządzenie DORA	Artykuły 5, 8, 9	ład wewnętrzny, ICT, zarządzanie incydentami obejmujące bezpieczeństwo fizyczne
COBIT 2019	DSS01, DSS05, MEA	zarządzane operacje, usługi bezpieczeństwa oraz monitorowanie zgodności

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe środki kontrolne służące ochronie informacji wrażliwych poprzez wymaganie bezpiecznego postępowania z dokumentami papierowymi, stacjami roboczymi, ekranami oraz nośnikami wymiennymi zarówno w środowisku biurowym, jak i we współdzielonych przestrzeniach pracy.

1.2 Wspiera ona Załącznik A do ISO/IEC 27001, środek kontrolny 7.7, poprzez egzekwowanie praktyk behawioralnych i technicznych ograniczających ryzyko nieuprawnionego ujawnienia, kradzieży lub utraty danych wskutek pozostawienia informacji bez nadzoru albo ich widoczności dla osób nieuprawnionych.

1.3 Polityka wzmacnia bezpieczeństwo fizyczne i bezpieczeństwo informacji w codziennej działalności oraz wspiera zgodność z mającymi zastosowanie obowiązkami prawnymi, umownymi i regulacyjnymi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do całego personelu przebywającego w fizycznych przestrzeniach roboczych lub uzyskującego do nich dostęp, w tym do:

2.1.1 pracowników stałych i personelu tymczasowego

2.1.2 wykonawców, konsultantów, dostawców i stażystów

2.1.3 zewnętrznych dostawców usług oraz osób odwiedzających na miejscu, które mają dostęp do informacji wrażliwych

2.2 Wymagania mają zastosowanie w:

2.2.1 indywidualnych biurach, boksach i otwartych przestrzeniach roboczych

2.2.2 salach spotkań i współdzielonych strefach współpracy

2.2.3 strefach drukarek, recepcjach i pomieszczeniach kopiowania

2.2.4 obszarach, w których wykorzystywane są zdalne stacje robocze lub współdzielone kioski

2.3 Niniejsza polityka ma również zastosowanie do tymczasowych lub hybrydowych środowisk pracy (np. hot-desking) oraz miejsc publicznie dostępnych, w których występuje ryzyko podglądu ekranu przez osoby postronne lub pozostawienia danych bez nadzoru.

3. Cele

3.1 Zapobieganie nieuprawnionemu dostępowi do informacji poufnych, wrażliwych lub regulowanych pozostawionych w formie fizycznej lub cyfrowej.

3.2 Promowanie spójnego poziomu ryzyka w obszarze bezpieczeństwa we wszystkich środowiskach pracy poprzez stosowanie zabezpieczeń fizycznych, właściwej konfiguracji stacji roboczych oraz odpowiednich zachowań użytkowników końcowych.

3.3 Ograniczenie ryzyka naruszeń prywatności, utraty własności intelektualnej oraz eksfiltracji danych spowodowanych zaniedbaniem lub przeoczeniem.

3.4 Utrwalenie zasad czystego biurka i czystego ekranu w kulturze organizacyjnej w celu wspierania dyscypliny operacyjnej, rozliczalności audytowej oraz zdolności do obrony w przypadku kontroli regulacyjnej.

3.5 Wspieranie zgodności z ISO/IEC 27001, art. 32 RODO, art. 15 Dyrektywy NIS2 oraz innymi wymaganiami bezpieczeństwa fizycznego dotyczącymi danych krytycznych lub danych osobowych.

4. Role i odpowiedzialności

4.1 Kadra kierownicza wyższego szczebla

4.1.1 Zatwierdza niniejszą politykę i promuje kulturę świadomości bezpieczeństwa we wszystkich jednostkach organizacyjnych.

4.1.2 Przydziela odpowiednie zasoby na stosowanie postanowień polityki, kampanie podnoszące świadomość oraz mechanizmy kontroli fizycznej.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO) / Menedżer systemu zarządzania bezpieczeństwem informacji

4.2.1 Odpowiada za niniejszą politykę i zapewnia jej zgodność z ISO/IEC 27001:2022, wymaganiami audytowymi oraz strategiami postępowania z ryzykiem.

4.2.2 Opracowuje programy podnoszenia świadomości i środki kontrolne zapewniające spójne wdrożenie we wszystkich obiektach oraz hybrydowych środowiskach pracy.

4.2.3 Koordynuje działania z zespołami administracji obiektami i IT w celu zapewnienia wdrożenia odpowiednich zabezpieczeń fizycznych.

[... 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 Harmonogram przeglądu polityki

9.1.1 Niniejsza polityka podlega przeglądowi:

9.1.1.1 co najmniej raz w roku

9.1.1.2 po każdej niezgodności audytowej związanej z ekspozycją przestrzeni roboczej lub ekranu

9.1.1.3 po incydencie fizycznym lub środowiskowym (np. kradzież urządzenia, tailgating, nadzór)

9.1.1.4 po wdrożeniu nowych układów biurowych, polityk obiektowych lub modeli organizacji pracy (np. hot-desking, zdalne huby)

9.2 Odpowiedzialni właściciele

9.2.1 Właścicielem polityki jest Dyrektor ds. bezpieczeństwa informacji (CISO) lub wyznaczony Menedżer systemu zarządzania bezpieczeństwem informacji.

9.2.2 Proces przeglądu obejmuje udział:

9.2.2.1 zespołów administracji obiektami i bezpieczeństwa korporacyjnego

9.2.2.2 IT i infrastruktury w zakresie wymuszania ustawień urządzeń

9.2.2.3 HR i działu prawnego w zakresie egzekwowania zachowań i spójności działań dyscyplinarnych

9.2.3 Wszystkie aktualizacje polityki muszą podlegać kontroli wersji, zostać zatwierdzone przez Komitet Sterujący SZBI oraz ponownie zakomunikowane wraz z wymaganym ponownym potwierdzeniem zapoznania się.

9.3 Komunikowanie zmian

9.3.1 Użytkownicy muszą być informowani o istotnych aktualizacjach za pośrednictwem:

9.3.1.1 repozytorium polityk w intranecie lub portalu

9.3.1.2 ukierunkowanej komunikacji e-mailowej

9.3.1.3 przypomnień onboardingowych i kwartalnych briefingów

9.3.1.4 obowiązkowych komunikatów o potwierdzeniu zapoznania się dla wszelkich nowych krytycznych klauzul dotyczących stosowania polityki

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest zgodna z następującymi dokumentami i je wspiera:

10.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia oczekiwania dotyczące zachowań użytkowników i bezpieczeństwa fizycznego stanowiące podstawę niniejszej polityki.

10.1.2 P3 – Polityka dopuszczalnego użytkowania: określa odpowiedzialność użytkowników za ochronę danych i systemów, w tym w środowiskach fizycznych.

10.1.3 P6 – Polityka zarządzania ryzykiem: uwzględnia ryzyka związane z fizyczną przestrzenią roboczą jako element analizy ryzyka informacyjnego w skali całej organizacji.

10.1.4 P12 – Polityka zarządzania aktywami: wspiera ewidencjonowanie i bezpieczne postępowanie z urządzeniami oraz nośnikami pozostawianymi na biurkach.

10.1.5 P13 – Polityka klasyfikacji danych i etykietowania: wiąże zasady czystego biurka z postępowaniem wobec dokumentów fizycznych oznaczonych jako Poufne lub Wewnętrzne.

10.1.6 P14 – Polityka retencji danych i utylizacji: określa zasady przechowywania dokumentów fizycznych, niszczenia i postępowania z pojemnikami.

10.1.7 P22 – Polityka rejestrowania i monitorowania: może być stosowana do monitorowania statusu blokady stacji roboczych, czasu bezczynności lub obrazu z kamer w przestrzeniach roboczych, tam gdzie jest to dozwolone.

10.2 Powiązane polityki tworzą zintegrowaną kulturę bezpieczeństwa, łącząc świadomość użytkowników, zabezpieczenia fizyczne i rozliczalność w celu zapewnienia odpornych przestrzeni roboczych.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z powszechnie uznanymi normami oraz wymaganiami prawnymi nakazującymi ochronę informacji wrażliwych w środowisku fizycznym i poprzez właściwe zachowania użytkowników.

11.2 ISO/IEC 27001

11.2.1 Klauzula 6.1.3 – plan postępowania z ryzykiem: wspiera wdrożenie środków kontrolnych ograniczających ryzyka fizyczne i środowiskowe, w tym te związane z zachowaniami użytkowników w otwartych przestrzeniach roboczych.

11.2.2 Klauzula 8.1 – planowanie operacyjne i nadzór: ustanawia zabezpieczenia operacyjne służące zarządzaniu bezpiecznymi przestrzeniami roboczymi i sposobem korzystania ze sprzętu.

11.3 ISO/IEC 27002:2022 – Środek kontrolny 7

11.3.1 Środek ten wymaga stosowania zabezpieczeń behawioralnych i kontroli środowiskowych zapobiegających nieuprawnionemu dostępowi do informacji za pośrednictwem nośników, ekranów lub materiałów drukowanych pozostawionych bez nadzoru. Niniejsza polityka egzekwuje higienę fizycznej przestrzeni roboczej, stosowanie blokady ekranu oraz utylizację dokumentów wrażliwych.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (uprawnienia dostępu fizycznego): powiązane z ograniczeniami przestrzeni roboczej i wymogiem zamykanego przechowywania w środowiskach wysokiego ryzyka.

11.4.2 PS-7 (bezpieczeństwo personelu zewnętrznego): stosowane poprzez rozszerzenie wymagań dotyczących czystego biurka i czystego ekranu na wykonawców i użytkowników stron trzecich.

11.4.3 MP-6 (sanityzacja nośników) oraz AC-11 (blokada sesji): realizowane poprzez procedury bezpiecznej utylizacji i obowiązkowe timery blokady ekranu.

11.4.4 CM-6 (ustawienia konfiguracyjne) oraz IA-5 (zarządzanie mechanizmami uwierzytelniającymi): wspierają techniczne wymuszanie blokowania ekranu i kontroli sesji na punktach końcowych.

11.5 RODO (2016/679)

11.5.1 Artykuł 5(1)(f): wymaga zapewnienia integralności i poufności danych osobowych, w tym ochrony przed fizyczną ekspozycją lub wglądem osób nieuprawnionych.

11.5.2 Artykuł 32 – bezpieczeństwo przetwarzania: wymaga stosowania odpowiednich środków fizycznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, utratą lub nieuprawnionym ujawnieniem — realizowane poprzez kontrole biurka i ekranu.

11.5.3 Motyw 39: wymaga ograniczenia dostępu do danych osobowych do osób uprawnionych — obejmuje to również ich zabezpieczenie w formie fizycznej, gdy pozostają bez nadzoru.

11.6 Dyrektywa NIS2 (2022/2555)

11.6.1 Artykuł 21(2)(d): wymaga polityk i procedur dotyczących bezpieczeństwa fizycznego i środowiskowego, w tym zabezpieczeń informacji na poziomie miejsca pracy.

11.6.2 Artykuł 21(3): promuje kulturę bezpieczeństwa obejmującą właściwe zachowania użytkowników, świadomość oraz zapobieganie niezamierzonym wyciekom danych — wspierane przez zabezpieczenia behawioralne określone w niniejszej polityce.

11.7 Rozporządzenie DORA (2022/2554)

11.7.1 Artykuł 5 – ład wewnętrzny i kontrola: wymaga, aby wszystkimi ryzykami związanymi z ICT, w tym zagrożeniami ludzkimi i środowiskowymi, zarządzano poprzez egzekwowalne polityki.

11.7.2 Artykuł 8 – zarządzanie ryzykiem ICT: wymaga zabezpieczeń zarówno w kontekście cyfrowym, jak i fizycznym, zapewniając, że użytkownicy zdalni, oddziałowi i korzystający z infrastruktury lokalnej nie tworzą niezarządzanej ekspozycji.

11.7.3 Artykuł 9 – zarządzanie incydentami: wymaga, aby uchybienia środowiskowe lub behawioralne prowadzące do ekspozycji danych były rejestrowane, klasyfikowane i obsługiwane z zastosowaniem odpowiednich działań korygujących.

11.8 COBIT 2019

11.8.1 DSS01 – zarządzane operacje: zapewnia dyscyplinę operacyjną w ochronie fizycznych przestrzeni roboczych i systemów poprzez powtarzalne środki kontrolne.

11.8.2 DSS05 – zarządzanie usługami bezpieczeństwa: wspiera ochronę danych, urządzeń i punktów dostępu poprzez oparte na zachowaniach stosowanie zasad, takich jak praktyki czystego biurka.

11.8.3 MEA03 – monitorowanie, ocena i zatwierdzanie modelu zgodności: wspiera audytowanie zabezpieczeń fizycznych i stosowania polityki w codziennych praktykach biznesowych.