					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P09S					Tytuł dokumentu: **Polityka pracy zdalnej**							
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 odpowiednich norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 6.1, 6.2, 8	
ISO/IEC 27002:2022	Środek kontrolny 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Dyrektywa NIS2	Artykuły 21(2)(b), 21(2)(h)	Dyrektywa UE NIS2
Rozporządzenie DORA	Artykuł 9	DORA UE
COBIT 2019	DSS05, APO13	COBIT 2019
RODO	Artykuł 32	RODO UE

1. Cel

1.1 Niniejsza polityka określa wymagania bezpieczeństwa dla pracowników i kontraktorów wykonujących pracę zdalną, w tym z domu, ze współdzielonych przestrzeni roboczych lub w trakcie podróży.

1.2 Jej celem jest ochrona poufności, integralności i dostępności (CIA) informacji biznesowych, do których uzyskuje się dostęp poza środowiskami kontrolowanymi przez organizację.

1.3 Niniejsza polityka zapewnia zgodność z odpowiednimi normami międzynarodowymi oraz ogranicza ryzyka, takie jak nieuprawniony dostęp, utrata danych i zakłócenia w świadczeniu usług.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich członków personelu (pracowników, kontraktorów, konsultantów oraz pracowników tymczasowych), którzy uzyskują dostęp do systemów, sieci lub danych organizacji podczas pracy poza siedzibą.

2.2 Obejmuje ona:

2.2.1 korzystanie z urządzeń wydanych przez organizację oraz urządzeń prywatnych,

2.2.2 dostęp za pośrednictwem VPN, pulpitu zdalnego lub usług chmurowych,

2.2.3 bezpieczne postępowanie z informacjami poza siedzibą organizacji,

2.2.4 monitorowanie, obsługę odstępstw oraz egzekwowanie postanowień.

2.3 Ma ona zastosowanie zarówno do pełnoetatowych, jak i niepełnoetatowych modeli pracy zdalnej, w tym do doraźnego dostępu zdalnego.

3. Cele

3.1 Zapobieganie nieuprawnionemu dostępowi do systemów organizacji lub danych wrażliwych podczas pracy zdalnej.

3.2 Zapewnienie, że urządzenia i łącza komunikacyjne używane poza biurem spełniają minimalne wymagania bezpieczeństwa.

3.3 Utrzymanie kontroli nad uprawnieniami dostępu zdalnego oraz monitorowaniem.

3.4 Zapewnienie pracownikom i kadrze kierowniczej jednoznacznych wytycznych dotyczących bezpiecznych praktyk pracy zdalnej.

3.5 Zapewnienie zgodności z wymaganiami ISO, NIS2, RODO, DORA i COBIT dotyczącymi pracy zdalnej i mobilnej.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny

4.1.1 Zatwierdza modele pracy zdalnej i nadzoruje zgodność.

4.1.2 Eskaluje incydenty bezpieczeństwa lub powtarzające się przypadki niezgodności.

4.1.3 Dokonuje przeglądu odstępstw i zapewnia realizację działań następczych po incydentach.

4.2 Dostawca wsparcia IT lub zewnętrzny dostawca usług IT

4.2.1 Konfiguruje bezpieczny dostęp zdalny (np. VPN, uwierzytelnianie wieloskładnikowe).

4.2.2 Zapewnia egzekwowanie ochrony punktów końcowych, szyfrowania oraz konfiguracji urządzeń.

4.2.3 Wspiera użytkowników i analizuje wszelkie techniczne problemy bezpieczeństwa.

[... 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 Coroczny przegląd polityki

9.1.1 Dyrektor Generalny oraz dostawca wsparcia IT muszą dokonywać corocznego przeglądu niniejszej polityki w celu dostosowania jej do zmian technologicznych, zmian kadrowych oraz zmian prawnych.

9.2 Przesłanki wcześniejszej aktualizacji

9.2.1 Natychmiastowy przegląd jest wymagany po:

9.2.1.1 poważnym incydencie bezpieczeństwa związanym z pracą zdalną,

9.2.1.2 zmianach wymagań NIS2, RODO lub DORA,

9.2.1.3 przejściu na nową technologię dostępu zdalnego (np. inną platformę VPN).

9.3 Kontrola wersji i archiwizacja

9.3.1 Wszystkie wersje niniejszej polityki muszą być:

9.3.1.1 opatrzone datą i zatwierdzone przez Dyrektora Generalnego,

9.3.1.2 oznaczone numerem wersji,

9.3.1.3 archiwizowane przez co najmniej trzy lata.

9.4 Komunikacja z personelem

9.4.1 Aktualizacje polityki muszą być komunikowane wszystkim użytkownikom zdalnym. W przypadku każdej istotnej zmiany wymagane jest potwierdzenie zapoznania się.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest powiązana z poniższymi dokumentami i je wspiera:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: określa, kto zatwierdza dostęp zdalny i sprawuje nad nim nadzór

10.1.2 P4S – Polityka kontroli dostępu: ustanawia zasady bezpiecznej konfiguracji dostępu zdalnego oraz procedury cofania uprawnień

10.1.3 P6S – Polityka zarządzania ryzykiem: obejmuje śledzenie i ocenę ryzyk związanych z dostępem poza siedzibą organizacji

10.1.4 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: szkoli użytkowników w zakresie ryzyk pracy zdalnej i dobrych praktyk

10.1.5 P30S – Polityka reagowania na incydenty: reguluje reakcję na incydenty związane z dostępem zdalnym, takie jak wyciek poświadczeń lub utrata urządzenia

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1 – planowanie oparte na ryzyku dla scenariuszy dostępu zdalnego

11.1.2 Klauzula 6.2 – określa obowiązki HR w kontekście pracy mobilnej i zdalnej

11.1.3 Klauzula 8.1 – planowanie operacyjne i kontrola procesów zdalnych

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 6.7 – zawiera praktyczne wytyczne dotyczące bezpieczeństwa pracy zdalnej i mobilnej

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – kontrola dostępu zdalnego, zabezpieczenia sesji i monitorowanie bezpieczeństwa

11.3.2 AC-2 – kontrola kont użytkowników pracujących poza siedzibą organizacji

11.4 RODO

11.4.1 Artykuł 32 – wymaga ochrony danych już w fazie projektowania i domyślnej ochrony, również w środowiskach zdalnych

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21(2)(b) – wymaga bezpiecznego korzystania z systemów sieci i informacji

11.5.2 Artykuł 21(2)(h) – przewiduje środki bezpieczeństwa związane z zasobami ludzkimi, w tym kontrole poza siedzibą organizacji

11.6 Rozporządzenie DORA

11.6.1 Artykuł 9 – wymaga, aby podmioty finansowe utrzymywały odporność ICT we wszystkich trybach operacyjnych, w tym przy dostępie zdalnym

11.7 COBIT 2019

11.7.1 DSS05 – Zarządzanie usługami bezpieczeństwa: obejmuje ochronę punktów końcowych i bezpieczne praktyki pracy zdalnej

11.7.2 APO13 – Zarządzanie bezpieczeństwem: zapewnia bezpieczne nadawanie dostępu oraz nadzór nad ryzykiem w zakresie dostępu mobilnego i zdalnego