					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P09					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**

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące bezpiecznej realizacji pracy zdalnej, w tym korzystania z systemów organizacji, dostępu do danych oraz wykonywania obowiązków służbowych poza siedzibą organizacji.

1.2 Zapewnia ona poufność, integralność i dostępność (CIA) aktywów informacyjnych, do których uzyskuje się dostęp zdalnie, oraz ustanawia środki kontrolne ograniczające ryzyka związane z rozproszonym środowiskiem pracy.

1.3 Polityka realizuje wymagania załącznika A do normy ISO/IEC 27001:2022, środka kontrolnego 6.7, poprzez wdrożenie zabezpieczeń technicznych i proceduralnych dostosowanych do warunków pracy zdalnej.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do całego personelu uprawnionego do pracy zdalnej, w tym do:

2.1.1 pracowników (zatrudnionych w pełnym lub niepełnym wymiarze czasu pracy oraz na podstawie umów kontraktowych),

2.1.2 zewnętrznych usługodawców, konsultantów i dostawców,

2.1.3 personelu tymczasowego oraz personelu realizującego zadania projektowe z zatwierdzonym dostępem zdalnym.

2.2 Polityka obejmuje:

2.2.1 dostęp do systemów informatycznych organizacji przez korporacyjną sieć VPN lub zatwierdzone narzędzia dostępu zdalnego,

2.2.2 przetwarzanie informacji wrażliwych i regulowanych poza bezpiecznymi obszarami,

2.2.3 korzystanie ze sprzętu należącego do organizacji lub z urządzeń prywatnych (BYOD),

2.2.4 zabezpieczenia fizyczne i dostęp logiczny w środowiskach zdalnych.

2.3 Polityka obowiązuje we wszystkich lokalizacjach geograficznych i strefach czasowych, w których organizacja dopuszcza pracę zdalną, niezależnie od tego, czy ma ona charakter stały, doraźny, czy jest realizowana w ramach zdarzeń związanych z ciągłością działania.

3. Cele

3.1 Zapewnienie, że wyłącznie osoby uprawnione mogą uzyskiwać zdalny dostęp do systemów wewnętrznych i informacji.

3.2 Zapewnienie stosowania szyfrowania, uwierzytelniania wieloskładnikowego oraz zabezpieczeń punktów końcowych we wszystkich ścieżkach dostępu zdalnego.

3.3 Utrzymanie odpowiedniego profilu ryzyka w obszarze bezpieczeństwa wobec zagrożeń takich jak phishing, złośliwe oprogramowanie, eksfiltracja danych oraz nieuprawnione udostępnienie systemów.

3.4 Uregulowanie zasad przesyłania, przechowywania i drukowania danych wrażliwych w środowiskach poza siedzibą organizacji.

3.5 Wdrożenie środków bezpieczeństwa fizycznego ograniczających widoczność ekranu i nieuprawnioną obserwację podczas sesji zdalnych.

3.6 Zapewnienie zgodności z międzynarodowymi wymaganiami regulacyjnymi dotyczącymi zdalnego dostępu do danych, w tym z RODO, NIS2 i DORA.

4. Role i odpowiedzialności

4.1 Kadra kierownicza

4.1.1 Zatwierdza niniejszą politykę oraz zapewnia zasoby niezbędne do jej stosowania i integracji z procesami HR, IT i bezpieczeństwa informacji.

4.1.2 Zatwierdza kryteria kwalifikacji do pracy zdalnej oraz zakres stosowania polityki w jednostkach biznesowych.

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

4.2.1 Odpowiada za politykę, jej utrzymanie oraz zapewnienie zgodności z profilem ryzyka i wymaganiami regulacyjnymi.

4.2.2 Określa środki kontrolne bezpieczeństwa dla dostępu zdalnego (np. szyfrowanie, ochrona punktów końcowych, limity bezczynności sesji).

4.2.3 Zatwierdza obsługę odstępstw i monitoruje skuteczność kontroli.

[... 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 Częstotliwość przeglądu

9.1.1 Niniejsza polityka musi być przeglądana co najmniej raz w roku lub częściej w przypadku:

9.1.1.1 wdrożenia nowych technologii dostępu zdalnego,

9.1.1.2 istotnego rozszerzenia modelu pracy zdalnej (np. inicjatyw związanych z pracą hybrydową),

9.1.1.3 pojawienia się nowych zagrożeń, podatności lub incydentów związanych ze środowiskami zdalnymi,

9.1.1.4 zmian w odpowiednich ramach prawnych lub regulacyjnych.

9.2 Właściciel i proces przeglądu

9.2.1 Właścicielem polityki jest CISO. Przegląd musi być koordynowany z:

9.2.1.1 IT i architekturą,

9.2.1.2 HR oraz administracją obiektów (w zakresie skutków operacyjnych i wymagań dotyczących przestrzeni roboczej),

9.2.1.3 inspektorem ochrony danych (w zakresie prywatności i transgranicznych zabezpieczeń danych).

9.2.2 Aktualizacje polityki muszą być:

9.2.2.1 zatwierdzane przez Komitet Sterujący SZBI,

9.2.2.2 komunikowane wszystkim objętym nimi pracownikom i kontraktorom,

9.2.2.3 uwzględniane w materiałach wdrożeniowych i szkoleniach przypominających.

9.3 Nadzór nad dokumentem i dystrybucja

9.3.1 Polityka musi zawierać kontrolę wersji, datę wejścia w życie oraz historię zmian.

9.3.2 Wersje wycofane z użycia muszą być przechowywane zgodnie z Polityką zarządzania dokumentacją (P14).

9.3.3 Wersje zaktualizowane muszą skutkować obowiązkowym ponownym potwierdzeniem zapoznania się z polityką przez użytkowników uprawnionych do pracy zdalnej.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka działa łącznie z:

10.1.1 P1 – P01 Polityka bezpieczeństwa informacji: ustanawia bazowe wymagania bezpiecznego postępowania z aktywami, mające zastosowanie we wszystkich środowiskach pracy, w tym zdalnych.

10.1.2 P3 – Polityka dopuszczalnego użytkowania: reguluje właściwe korzystanie z urządzeń i systemów organizacji podczas sesji pracy zdalnej.

10.1.3 P4 – Polityka kontroli dostępu: zapewnia, że uprawnienia dostępu zdalnego są zgodne z zasadą najmniejszych uprawnień i właściwymi mechanizmami uwierzytelniania.

10.1.4 P6 – Polityka zarządzania ryzykiem: określa sposób identyfikacji, postępowania i monitorowania ryzyk związanych z pracą zdalną w ramach SZBI.

10.1.5 P12 – Polityka zarządzania aktywami: wymaga prowadzenia inwentaryzacji i zarządzania konfiguracją wszystkich urządzeń wykorzystywanych zdalnie.

10.1.6 P22 – Polityka rejestrowania i monitorowania: zapewnia, że sesje zdalne są monitorowane, podlegają audytowi i są przechowywane zgodnie z wymaganiami zgodności.

10.1.7 P14 – Polityka retencji i utylizacji danych: określa zasady postępowania z danymi istotne dla pracy zdalnej, w tym w odniesieniu do nośników wymiennych i utylizacji urządzeń.

10.2 Łącznie polityki te zapewniają, że praca zdalna jest bezpieczna, zgodna i egzekwowalna we wszystkich funkcjach i lokalizacjach geograficznych.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo ramami bezpieczeństwa, ochrony danych i zarządzania ryzykiem ICT, aby zapewnić bezpieczne, audytowalne i zgodne praktyki pracy zdalnej.

11.2 ISO/IEC 27001

11.2.1 Klauzula 6.1.3 – planowanie postępowania z ryzykiem: niniejsza polityka wspiera postępowanie z ryzykiem związanym z dostępem zdalnym i rozproszonym środowiskiem pracy.

11.2.2 Klauzula 8.1 – planowanie operacyjne i nadzór: wymaga wdrożenia środków kontrolnych dla systemów, do których uzyskuje się dostęp poza siedzibą organizacji.

11.2.3 Załącznik A, środek kontrolny 6.7 – praca zdalna: niniejsza polityka w pełni obejmuje wymagane środki kontrolne bezpieczeństwa informacji dla personelu wykonującego pracę poza siedzibą organizacji, w tym zabezpieczenia fizyczne i logiczne, nadzór nad dostępem oraz monitorowanie zachowań użytkowników.

11.3 ISO/IEC 27002:2022 – Środek kontrolny 6

11.3.1 Środek ten wymaga proceduralnych i technicznych zabezpieczeń dla pracy zdalnej. Obejmuje wymagania dotyczące bezpieczeństwa urządzeń, metod dostępu, postępowania z danymi, zabezpieczeń środowiskowych oraz zarządzania udziałem stron trzecich — wszystkie te wymagania są egzekwowane przez niniejszą politykę.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (dostęp zdalny): realizowany bezpośrednio przez kontrole VPN, uwierzytelnianie wieloskładnikowe, rejestrowanie sesji oraz autoryzację dostępu opartego na rolach dla użytkowników zdalnych.

11.4.2 AC-2 (zarządzanie kontami): reguluje kwalifikację dostępową, przypisywanie uprawnień zdalnych oraz dezaktywację kont.

11.4.3 SC-12 do SC-13 (ochrona kryptograficzna, ustanawianie kluczy kryptograficznych): realizowane poprzez obowiązkowe stosowanie VPN i szyfrowanie pełnodyskowe dla zdalnych punktów końcowych.

11.4.4 MP-5 (ochrona transportu nośników) oraz PE-18 (lokalizacja komponentów systemów informatycznych): wytyczne dotyczące pracy zdalnej wymagają ochrony transportu oraz zabezpieczeń fizycznych w środowiskach poza siedzibą organizacji.

11.4.5 AU-2, AU-6: rejestrowanie i monitorowanie sesji zdalnych wspiera wymagania w zakresie audytu i reagowania na incydenty.

11.5 RODO (2016/679)

11.5.1 Artykuł 32 – bezpieczeństwo przetwarzania: niniejsza polityka wymusza bezpieczeństwo dostępu zdalnego, szyfrowanie oraz środki kontrolne rejestrowania niezbędne do ochrony danych osobowych, do których uzyskuje się dostęp lub które są przetwarzane zdalnie.

11.5.2 Artykuł 5(1)(f): zapewnia, że dane osobowe, do których uzyskuje się dostęp poza siedzibą organizacji, są chronione przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą.

11.5.3 Motyw 39: podkreśla ograniczenie dostępu, integralność i poufność — szczególnie istotne, gdy urządzenia opuszczają bezpieczne obszary.

11.6 Dyrektywa NIS2 (2022/2555)

11.6.1 Artykuł 21(2)(a, b, d): wymaga zabezpieczenia dostępu zdalnego jako części organizacyjnych ram zarządzania ryzykiem ICT. Niniejsza polityka spełnia wymaganie dotyczące środków bezpieczeństwa obejmujących kontrolę dostępu, bezpieczeństwo danych oraz polityki organizacyjne dla środowisk zdalnych.

11.6.2 Artykuł 21(3): wspiera budowanie świadomości bezpieczeństwa i stosowanie polityk wśród personelu pracującego poza centralnymi lokalizacjami.

11.7 Rozporządzenie DORA (2022/2554)

11.7.1 Artykuł 5 – ład zarządczy i ramy kontroli wewnętrznej: niniejsza polityka wspiera oczekiwania dotyczące kontroli ryzyka ICT we wszystkich scenariuszach operacyjnych, w tym w modelach hybrydowych i zdalnych.

11.7.2 Artykuł 8 – ramy zarządzania ryzykiem ICT: ryzyka dostępu zdalnego są tutaj identyfikowane, ograniczane i objęte nadzorem przy użyciu zabezpieczeń technicznych i organizacyjnych.

11.7.3 Artykuł 9 – uzgodnienia dotyczące wymiany informacji: chroni przed zdalnym wyciekiem informacji udostępnianych w sieciach cyfrowej odporności operacyjnej.

11.8 COBIT 2019

11.8.1 DSS01 – zarządzane operacje: niniejsza polityka wspiera bezpieczną ciągłość operacji biznesowych niezależnie od lokalizacji fizycznej.

11.8.2 BAI06 – zarządzane zmiany IT oraz BAI09 – zarządzane aktywa: zapewniają, że urządzenia wykorzystywane do pracy zdalnej są śledzone, bezpiecznie skonfigurowane i traktowane jako aktywa krytyczne.

11.8.3 APO13 – zarządzane bezpieczeństwo: promuje zdefiniowane ramy ładu bezpieczeństwa dla środowisk zdalnych.

11.8.4 MEA03 – monitorowanie, ocena i ocena zgodności: ustanawia wymóg, aby aktywność związana z pracą zdalną była rejestrowana, przeglądana i audytowana.