					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P03S					Tytuł dokumentu: **Polityka dopuszczalnego użytkowania**							
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, tam gdzie ma to zastosowanie

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 5	Istotne dla ogólnego zakresu polityki i jej wdrożenia
ISO/IEC 27002:2022	5.10, 5.11, 5	Wytyczne dotyczące wymagań i zabezpieczeń w zakresie dopuszczalnego użytkowania
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Obejmuje korzystanie z systemów i urządzeń, monitorowanie oraz szkolenie użytkowników
RODO	Artykuły 5 ust. 1 lit. f, 32	Integralność, poufność danych oraz środki bezpieczeństwa
Dyrektywa NIS2	Artykuł 21 ust. 2 lit. b	Wymaga odpowiednich polityk bezpieczeństwa, w tym zasad dopuszczalnego użytkowania
Rozporządzenie DORA	Artykuł 9	Polityka zarządzania ryzykiem ICT, zabezpieczenia oraz egzekwowanie postanowień
COBIT 2019	DSS05, BAI	Usługi bezpieczeństwa i zarządzanie wiedzą

1. Cel

1.1. Niniejsza polityka określa zasady dopuszczalnego, odpowiedzialnego i bezpiecznego korzystania z systemów, urządzeń, dostępu do Internetu, poczty elektronicznej, usług chmury obliczeniowej oraz wszelkich urządzeń prywatnych wykorzystywanych do celów służbowych.

1.2. Zapewnia, że użytkownicy rozumieją swoje obowiązki podczas korzystania z zasobów informatycznych organizacji, chroniąc integralność danych, prywatność oraz ciągłość operacyjną.

1.3. Niniejsza polityka wspiera zgodność z ISO/IEC 27001:2022 poprzez ustanowienie jasnych standardów zachowania użytkowników, zgodnych z wymaganiami prawnymi, umownymi i regulacyjnymi.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich osób, które uzyskują dostęp do systemów lub danych organizacji, zarządzają nimi lub z nich korzystają, w tym:

2.1.1. pracowników i współpracowników

2.1.2. pracowników tymczasowych i stażystów

2.1.3. zewnętrznych dostawców usług IT

2.2. Obejmuje ona:

2.2.1. komputery, telefony i tablety stanowiące własność organizacji

2.2.2. urządzenia prywatne dopuszczone do użytku służbowego (BYOD)

2.2.3. sieci organizacji, platformy chmury obliczeniowej oraz usługi programowe

2.2.4. dostęp do Internetu, systemy poczty elektronicznej, współdzielone zasoby pamięci masowej oraz aplikacje biznesowe

2.3. Niniejsza polityka obowiązuje we wszystkich środowiskach pracy — stacjonarnym, zdalnym i hybrydowym — oraz przez cały czas wykonywania obowiązków służbowych.

3. Cele

3.1. Określenie, co stanowi dopuszczalne i niedopuszczalne korzystanie z systemów IT.

3.1.1. Ograniczenie ryzyk bezpieczeństwa wynikających z niewłaściwego użytkowania, nieuprawnionego dostępu lub wprowadzenia złośliwego oprogramowania.

3.1.2. Ochrona danych biznesowych, informacji o klientach oraz reputacji organizacji.

3.1.3. Ustanowienie egzekwowalnych zasad i zapewnienie rozliczalności wszystkich użytkowników.

3.1.4. Wsparcie monitorowania i zgodności w celu wczesnego wykrywania naruszeń oraz podejmowania działań korygujących.

4. Role i obowiązki

4.1. Dyrektor Generalny

4.1.1. Zatwierdza niniejszą politykę i odpowiada za zapewnienie zasobów oraz uprawnień niezbędnych do jej stosowania.

4.1.2. Dokonuje przeglądu i zatwierdza wszelkie odstępstwa od niniejszej polityki.

4.2. Kierownik IT lub zewnętrzny dostawca usług IT

4.2.1. Utrzymuje wykazy zatwierdzonego oprogramowania i sprzętu.

4.2.2. Konfiguruje urządzenia w sposób zapewniający egzekwowanie zasad dopuszczalnego użytkowania (np. filtrowanie treści, rejestrowanie dostępu).

4.2.3. Monitoruje wykorzystanie pod kątem potencjalnych naruszeń i prowadzi analizę incydentów.

4.2.4. Zapewnia, że urządzenia prywatne (BYOD), jeżeli są wykorzystywane służbowo, są autoryzowane i odpowiednio zabezpieczone.

[... 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

9.1.1. Niniejsza polityka musi podlegać corocznemu przeglądowi przez Kierownika IT, z końcowym zatwierdzeniem przez Dyrektora Generalnego, aby zapewnić jej zgodność ze sposobami wykorzystania technologii, nowymi ryzykami oraz obowiązkami w zakresie zgodności.

9.2. Przesłanki przeglądu doraźnego

9.2.1. Przeglądy muszą być również przeprowadzane w odpowiedzi na:

9.2.2. nowe systemy lub technologie (np. nową usługę chmury obliczeniowej lub platformę urządzeń końcowych)

9.2.3. istotne naruszenia polityki

9.2.4. zaktualizowane przepisy prawa lub warunki umowne wpływające na korzystanie z IT

9.3. Dokumentowanie zmian

9.3.1. Wszystkie aktualizacje muszą być rejestrowane w rejestrze wersji obejmującym:

9.3.1.1. numer wersji

9.3.1.2. datę przeglądu

9.3.1.3. podsumowanie zmian

9.3.1.4. organ zatwierdzający

9.4. Komunikowanie polityki

9.4.1. Zmienione wersje niniejszej polityki muszą zostać przekazane wszystkim użytkownikom, których dotyczą. Pracownicy muszą potwierdzić ich otrzymanie i zrozumienie w ramach swoich obowiązków w zakresie świadomości bezpieczeństwa.

10. Powiązane polityki i zależności

10.1. Niniejsza polityka funkcjonuje łącznie z innymi politykami SME, aby zapewnić kompleksowe ujęcie odpowiedzialności w zakresie bezpieczeństwa:

10.1.1. P4S – Polityka kontroli dostępu: określa techniczne i proceduralne stosowanie zasad dozwolonego użytkowania oraz ograniczeń dotyczących kont.

10.1.2. P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia użytkownikom edukację dotyczącą granic dopuszczalnego użytkowania oraz obowiązków zgłaszania.

10.1.3. P9S – Polityka pracy zdalnej: reguluje korzystanie z systemów organizacji poza siedzibą lub w środowisku domowym.

10.1.4. P17S – Polityka ochrony danych i prywatności: określa zasady postępowania z danymi osobowymi, które pozostają powiązane z monitorowaniem dopuszczalnego użytkowania oraz BYOD.

10.1.5. P30S – Polityka reagowania na incydenty: reguluje procedury badania przypadków niewłaściwego użytkowania lub naruszeń zasad dopuszczalnego użytkowania oraz reagowania na nie.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001

11.1.1. Klauzula 5.10 – wymaga, aby organizacje określały i egzekwowały dopuszczalne użytkowanie aktywów organizacji.

11.2. ISO/IEC 27002

11.2.1. Zabezpieczenie 5.10 – zawiera wytyczne dotyczące dopuszczalnego użytkowania systemów, w tym zachowań dozwolonych i zabronionych.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – dotyczy kontroli korzystania z systemów, w tym wykorzystywania prywatnych urządzeń (BYOD).

11.3.2. AC-20 – wymaga autoryzacji i monitorowania systemów zewnętrznych.

11.3.3. AT-2 – podkreśla znaczenie szkolenia użytkowników w zakresie praktyk dopuszczalnego użytkowania.

11.4. RODO

11.4.1. Artykuł 5 ust. 1 lit. f – wymaga zapewnienia integralności i poufności danych osobowych, które mogą zostać naruszone wskutek niewłaściwego użytkowania przez użytkownika.

11.4.2. Artykuł 32 – wymaga wdrożenia środków technicznych i organizacyjnych w celu zabezpieczenia systemów i danych.

11.5. Dyrektywa NIS2

11.5.1. Artykuł 21 ust. 2 lit. b – wymaga odpowiednich polityk bezpieczeństwa, w tym zasad dopuszczalnego użytkowania, w celu ograniczania cyberzagrożeń.

11.6. Rozporządzenie DORA

11.6.1. Artykuł 9 – wymaga polityk zarządzania ryzykiem ICT, obejmujących kontrole użytkowania oraz mechanizmy egzekwowania postanowień.

11.7. COBIT 2019

11.7.1. DSS05 – Zarządzanie usługami bezpieczeństwa: podkreśla znaczenie opartej na politykach kontroli zachowań użytkowników.

11.7.2. BAI08 – Zarządzanie wiedzą: odnosi się do świadomości obowiązków wynikających z polityk oraz edukacji w zakresie dopuszczalnego użytkowania.