					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P20S					Tytuł dokumentu: **Polityka ochrony punktów końcowych przed złośliwym oprogramowaniem**							
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**

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.
Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.
W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do odpowiednich norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	Środki kontroli operacyjnej dotyczące ochrony przed złośliwym oprogramowaniem
ISO/IEC 27002:2022	Środek kontroli 8	Środki kontroli dotyczące ochrony punktów końcowych
NIST SP 800-53 Rev.5	SI-3, SI-4	Ochrona przed złośliwym kodem i reagowanie na incydenty
Dyrektywa UE NIS2	Artykuły 21(2)(d), (e)	Ochrona przed złośliwym oprogramowaniem i zarządzanie ryzykiem dla podmiotów kluczowych i ważnych
Rozporządzenie UE DORA	Artykuły 10(1), 15	Odporność operacyjna i weryfikacja podmiotów trzecich
COBIT 2019	DSS05.02, DSS05.04	Ochrona punktów końcowych i sieci oraz monitorowanie
RODO	Artykuły 32(1)(b), 33	Środki techniczne i organizacyjne oraz zgłaszanie naruszeń

1. Cel

1.1 Niniejsza polityka określa minimalne wymagania techniczne, proceduralne i behawioralne dotyczące ochrony wszystkich urządzeń końcowych — takich jak laptopy, komputery stacjonarne, urządzenia mobilne i nośniki przenośne — przed złośliwym kodem, w tym wirusami, ransomware, spyware, rootkitami oraz innymi zagrożeniami związanymi ze złośliwym oprogramowaniem.

1.2 Celem polityki jest zapewnienie, że punkty końcowe są wyposażane, utrzymywane i użytkowane w sposób ograniczający ryzyko infekcji złośliwym oprogramowaniem, jego rozprzestrzeniania się oraz naruszenia bezpieczeństwa systemów.

1.3 Organizacja uznaje, że punkty końcowe są częstym wektorem wejścia dla złośliwego oprogramowania, dlatego muszą być odpowiednio utwardzane, monitorowane i chronione z wykorzystaniem wielowarstwowych mechanizmów obronnych.

1.4 Polityka wspiera cele organizacji związane z certyfikacją ISO/IEC 27001:2022 oraz pozostaje zgodna z RODO, Dyrektywą NIS2, Rozporządzeniem DORA oraz innymi właściwymi ramami odniesienia.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich organizacyjnych punktów końcowych, w tym komputerów stacjonarnych, laptopów, tabletów, telefonów komórkowych oraz terminali punktów sprzedaży

2.1.2 urządzeń prywatnych (BYOD) wykorzystywanych do uzyskiwania dostępu do aplikacji biznesowych lub danych

2.1.3 wymiennych nośników danych, takich jak pamięci USB i zewnętrzne dyski twarde

2.1.4 wszelkich systemów operacyjnych, aplikacji dla punktów końcowych oraz narzędzi komunikacyjnych działających na tych platformach

2.2 Polityka ma jednakowe zastosowanie do:

2.2.1 pracowników, wykonawców, stażystów oraz dostawców usług zarządzanych

2.2.2 urządzeń używanych lokalnie, zdalnie lub w modelu pracy hybrydowej

2.2.3 punktów końcowych połączonych z chmurą lub działających offline, przechowujących dane biznesowe lub dane osobowe

3. Cele

3.1 Zapobieganie infekcjom złośliwym oprogramowaniem i jego rozprzestrzenianiu się w systemach wewnętrznych, na urządzeniach użytkowników oraz za pośrednictwem połączeń zewnętrznych

3.2 Szybkie wykrywanie i ograniczanie zagrożeń związanych ze złośliwym oprogramowaniem przy użyciu zautomatyzowanych technologii ochrony punktów końcowych oraz określonych ścieżek eskalacji

3.3 Zapewnienie, że do dostępu do informacji biznesowych wykorzystywane są wyłącznie urządzenia autoryzowane, zabezpieczone i monitorowane

3.4 Określenie jednoznacznych odpowiedzialności personelu i zasad postępowania użytkowników w celu ograniczenia ryzyka incydentów związanych ze złośliwym oprogramowaniem

3.5 Utrzymywanie możliwych do prześledzenia w audycie zapisów dotyczących wykrycia złośliwego oprogramowania, reakcji na nie oraz zgodności z polityką

3.6 Ochrona danych osobowych i danych biznesowych przed naruszeniem bezpieczeństwa wskutek działania złośliwego oprogramowania z wykorzystaniem strategii ochrony wielowarstwowej

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Odpowiada za niniejszą politykę i zapewnia dostępność wystarczających zasobów na potrzeby ochrony punktów końcowych

4.1.2 Zatwierdza oprogramowanie antywirusowe, narzędzia do zarządzania urządzeniami mobilnymi (MDM) oraz zasady dostępu podmiotów trzecich

4.1.3 Przegląda raporty dotyczące incydentów związanych ze złośliwym oprogramowaniem, podsumowania wpływu oraz zgłoszenia naruszeń dotyczących punktów końcowych

4.2 Dostawca wsparcia IT / wewnętrzny administrator IT

4.2.1 Wybiera i wdraża oprogramowanie antywirusowe, antymalware oraz rozwiązania EDR (Endpoint Detection and Response)

4.2.2 Zapewnia spójne wdrażanie aktualizacji oraz przechowywanie logów

4.2.3 Reaguje na alerty dotyczące złośliwego oprogramowania, izoluje zainfekowane systemy i prowadzi działania naprawcze

4.2.4 Egzekwuje środki kontroli dotyczące korzystania z urządzeń USB i urządzeń zewnętrznych

[... 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 Wymóg corocznego przeglądu

9.1.1 Niniejsza polityka musi podlegać formalnemu przeglądowi co najmniej raz w roku przez Dyrektora Generalnego, we współpracy z Dostawcą wsparcia IT oraz Koordynatorem ds. prywatności

9.2 Aktualizacje inicjowane zdarzeniami

9.2.1 Aktualizacje polityki muszą być również przeprowadzane, gdy:

9.2.1.1 nowe istotne zagrożenie lub fala ataków z użyciem złośliwego oprogramowania jest wymierzona w punkty końcowe wykorzystywane przez organizację

9.2.1.2 narzędzia antywirusowe lub EDR zostają zmienione, zmodernizowane lub zastąpione

9.2.1.3 incydent związany ze złośliwym oprogramowaniem ujawni słabości w zakresie lub stosowaniu niniejszej polityki

9.2.1.4 zaktualizowane zostaną wymagania prawne lub regulacyjne, np. RODO, DORA, NIS2

9.3 Kontrola wersji i komunikacja

9.3.1 Wszystkie zmiany polityki muszą być dokumentowane z numerem wersji, datą oraz podsumowaniem zmian

9.3.2 Personel musi zostać poinformowany o aktualizacjach, zwłaszcza jeżeli zmieniają one wymagania operacyjne lub behawioralne

9.3.3 Poprzednie wersje muszą być przechowywane w archiwum polityk przez co najmniej 3 lata w celu wsparcia audytów

10. Powiązane polityki i zależności

10.1 Niniejsza polityka musi być wdrażana łącznie z następującymi politykami SME:

10.1.1 P9S – Polityka pracy zdalnej: zapewnia stosowanie wymagań ochrony punktów końcowych na urządzeniach używanych poza siedzibą organizacji lub w modelu hybrydowym

10.1.2 P12S – Polityka zarządzania aktywami: wspiera ewidencję i kontrolę wszystkich punktów końcowych, zapewniając wykorzystywanie wyłącznie urządzeń autoryzowanych i chronionych

10.1.3 P17S – Polityka ochrony danych i prywatności: wzmacnia zapobieganie złośliwemu oprogramowaniu jako kluczowy środek ochrony prywatności służący zabezpieczeniu danych osobowych i danych wrażliwych przed naruszeniem bezpieczeństwa

10.1.4 P22S – Polityka logowania i monitorowania: określa wymagania dotyczące rejestrowania zdarzeń związanych ze złośliwym oprogramowaniem oraz utrzymywania widoczności alertów na potrzeby wczesnej reakcji

10.1.5 P30S – Polityka reagowania na incydenty: określa etapy eskalacji, ograniczania skutków oraz notyfikacji zewnętrznych, jeżeli złośliwe oprogramowanie prowadzi do naruszenia danych lub zakłócenia działalności operacyjnej

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – Wymaga wdrożenia środków kontroli operacyjnej w celu ograniczenia ryzyk, takich jak ataki z użyciem złośliwego oprogramowania

11.2 ISO/IEC 27002

11.2.1 Środek kontroli 8.7 – Opisuje praktyki kontroli złośliwego oprogramowania, w tym antywirus, skanowanie w czasie rzeczywistym, aktualizacje i szkolenia użytkowników

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Wymaga wdrożenia mechanizmów ochrony przed złośliwym kodem na punktach końcowych

11.3.2 SI-4 – Nakłada obowiązek monitorowania, wykrywania, analizy oraz podejmowania działań reakcyjnych wobec zagrożeń i alertów na poziomie punktu końcowego

11.4 RODO

11.4.1 Artykuł 32(1)(b) – Wymaga technicznych i organizacyjnych środków kontroli, takich jak antywirus, w celu ochrony danych osobowych

11.4.2 Artykuł 33 – Nakłada obowiązek zgłoszenia naruszenia, gdy złośliwe oprogramowanie narusza integralność, poufność lub dostępność danych

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21(2)(d) – Wymaga środków zapobiegających zagrożeniom związanym ze złośliwym oprogramowaniem i reagowania na nie w podmiotach kluczowych i ważnych

11.5.2 Artykuł 21(2)(e) – Nakłada obowiązek stosowania warstwowych strategii zarządzania ryzykiem cyberbezpieczeństwa, w tym ochrony punktów końcowych przed złośliwym oprogramowaniem

11.6 Rozporządzenie UE DORA

11.6.1 Artykuł 10(1) – Wymaga ochrony systemów ICT przed złośliwym oprogramowaniem i innymi zagrożeniami w ramach odporności operacyjnej

11.6.2 Artykuł 15 – Nakłada na organizacje finansowe obowiązek weryfikacji ochrony przed złośliwym oprogramowaniem u dostawców usług będących podmiotami trzecimi

11.7 COBIT 2019

11.7.1 DSS05.02 – Podkreśla znaczenie środków ochrony służących zabezpieczeniu punktów końcowych i sieci przed zagrożeniami związanymi ze złośliwym oprogramowaniem

11.7.2 DSS05.04 – Wspiera monitorowanie i alertowanie w odniesieniu do zdarzeń bezpieczeństwa związanych ze złośliwym oprogramowaniem w ramach bieżących operacji