					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P20					Tytuł dokumentu: **Polityka ochrony punktów końcowych / ochrony 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**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	Wymagane są zabezpieczenia punktów końcowych oraz środki ochrony przed złośliwym oprogramowaniem w celu realizacji celów SZBI
ISO/IEC 27002:2022	Środki kontrolne 8.7, 8	Określa zabezpieczenia techniczne i wytyczne dotyczące ochrony przed złośliwym oprogramowaniem, ochrony punktów końcowych oraz obsługi incydentów
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Określa wymagania dotyczące ochrony przed złośliwym kodem, scentralizowanego monitorowania oraz konfiguracji bazowej
RODO UE	Artykuł 32	Wymaga wdrożenia odpowiednich środków technicznych w celu ochrony danych osobowych, w tym ochrony przed złośliwym oprogramowaniem
NIS2 UE	Artykuł 21(2)(d)	Wymaga wdrożenia mechanizmów wykrywania zagrożeń oraz środków zapobiegawczych na poziomie punktów końcowych
DORA UE	Artykuł 9	Wymaga zarządzania ryzykiem ICT w zakresie ochrony przed złośliwym oprogramowaniem i zagrożeniami przenoszonymi przez punkty końcowe
COBIT 2019	DSS05.01, DSS01.04, MEA	Wymaga ochrony, monitorowania i oceny zabezpieczeń punktów końcowych

1. Cel

1.1 Niniejsza polityka określa obowiązkowe zabezpieczenia i wymagania operacyjne dotyczące ochrony organizacyjnych punktów końcowych — w tym stacji roboczych, laptopów, urządzeń mobilnych i serwerów — przed złośliwym oprogramowaniem oraz powiązanymi zagrożeniami.

1.2 Ustanawia minimalne wymagania w zakresie ochrony punktów końcowych, wykrywania złośliwego oprogramowania, działań powstrzymujących oraz monitorowania behawioralnego, tak aby systemy zachowywały odporność zarówno na powszechne, jak i zaawansowane odmiany złośliwego oprogramowania.

1.3 Polityka bezpośrednio wspiera zgodność z ISO/IEC 27001:2022, klauzulą 8.1 oraz załącznikiem A, środkiem kontrolnym 8.7, i jest zgodna z regionalnymi obowiązkami w zakresie cyberbezpieczeństwa wynikającymi z RODO, NIS2 i DORA.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich punktów końcowych, w tym:

2.1.1 stacji roboczych, laptopów, urządzeń mobilnych i instancji wirtualnych będących własnością organizacji lub przez nią zarządzanych,

2.1.2 urządzeń prywatnych dopuszczonych zgodnie z Polityką BYOD (z zastrzeżeniem wdrożenia MDM lub agenta punktu końcowego),

2.1.3 serwerów i zasobów infrastrukturalnych, w tym maszyn wirtualnych hostowanych w chmurze oraz urządzeń brzegowych,

2.1.4 systemów operacyjnych, sterowników, usług lokalnych, agentów punktów końcowych oraz zabezpieczeń zainstalowanych na każdym węźle.

2.2 Niniejsza polityka obejmuje cały personel ponoszący odpowiedzialność administracyjną, techniczną lub operacyjną za dowolny punkt końcowy, w tym:

2.2.1 pracowników wewnętrznych i wykonawców,

2.2.2 dostawców usług zarządzanych (MSP), zespoły wsparcia stacji roboczych świadczone w modelu outsourcingowym oraz administratorów IT stron trzecich,

2.2.3 użytkowników uprawnionych do korzystania z systemów przenośnych, laptopów z dostępem VPN lub mobilnym dostępem do sieci organizacji.

2.3 Zakres zagrożeń objętych niniejszą polityką obejmuje w szczególności:

2.3.1 wirusy, robaki, trojany, ransomware, spyware, rootkity, adware, keyloggery, botnety,

2.3.2 złośliwe oprogramowanie bezplikowe, ładunki typu zero-day, złośliwe oprogramowanie służące do eskalacji uprawnień oraz zestawy exploitów przeglądarkowych,

2.3.3 złośliwy kod dostarczany za pośrednictwem nośników wymiennych, wektorów phishingowych, pobrań typu drive-by lub ataków z użyciem USB.

3. Cele

3.1 Chronić integralność, dostępność i poufność systemów punktów końcowych oraz przetwarzanych przez nie danych poprzez skuteczne zapobieganie złośliwemu oprogramowaniu, jego wykrywanie oraz reagowanie.

3.2 Zapobiegać uruchomieniu lub rozprzestrzenianiu się złośliwego kodu w sieciach organizacji poprzez stosowanie zabezpieczeń technicznych, utwardzonej konfiguracji bazowej oraz telemetrii w czasie rzeczywistym.

3.3 Zintegrować ochronę punktów końcowych z innymi zabezpieczeniami SZBI, w tym z zarządzaniem podatnościami, kontrolą dostępu, rejestrowaniem i monitorowaniem oraz reagowaniem na incydenty.

3.4 Zapewnić ciągłą widoczność punktów końcowych za pośrednictwem centralnie zarządzanych platform ochronnych, w tym agentów antywirusowych/antymalware, systemów wykrywania i reagowania na punktach końcowych (EDR) oraz telemetrii SIEM.

3.5 Zapewnić zgodność z wymaganiami prawnymi, regulacyjnymi i normatywnymi dotyczącymi bezpieczeństwa punktów końcowych (np. art. 32 RODO, art. 21 NIS2, art. 9 DORA).

3.6 Określić role odpowiedzialne, egzekwować SLA dla wdrażania poprawek i obsługi alertów oraz zapewnić gotowość audytową poprzez dokumentowanie i raportowanie.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia jej zgodność z SZBI oraz ogólną strategią bezpieczeństwa.

4.1.2 Dokonuje kwartalnego przeglądu wskaźników ochrony punktów końcowych, trendów incydentów oraz skuteczności narzędzi.

4.1.3 Zatwierdza odstępstwa oraz akceptację ryzyka rezydualnego związaną z zakresem ochrony punktów końcowych.

4.2 Kierownik ds. Bezpieczeństwa Punktów Końcowych / Kierownik SOC

4.2.1 Zarządza systemami ochrony punktów końcowych (np. AV, EDR, MDM).

4.2.2 Nadzoruje stosowanie polityki, strojenie mechanizmów wykrywania zagrożeń oraz procedury operacyjne reagowania na incydenty.

4.2.3 Utrzymuje statystyki pokrycia, rejestry incydentów złośliwego oprogramowania oraz bazowe konfiguracje alertów.

[... 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 Niniejsza polityka musi podlegać przeglądowi co najmniej raz w roku lub gdy:

9.1.1 wystąpią istotne kampanie złośliwego oprogramowania lub incydenty bezpieczeństwa dotyczące punktów końcowych,

9.1.2 nowe typy zagrożeń (np. złośliwe oprogramowanie bezplikowe, warianty ransomware) wymagają aktualizacji strategii wykrywania lub reagowania,

9.1.3 platformy ochrony punktów końcowych lub architektury agentów ulegną istotnym zmianom,

9.1.4 zostaną zaktualizowane wymagania prawne lub regulacyjne wpływające na zabezpieczenia punktów końcowych.

9.2 Przegląd inicjuje Kierownik ds. Bezpieczeństwa Punktów Końcowych i koordynuje go z CISO oraz funkcjami prawną, ryzyka i audytu.

9.3 Zatwierdzone zmiany muszą być udokumentowane w rejestrze kontroli dokumentów SZBI, otrzymać nowy identyfikator wersji i zostać zakomunikowane wszystkim zainteresowanym stronom.

9.4 Wersje wycofane z użycia muszą być archiwizowane, objęte ograniczeniami dostępu i przechowywane dla zachowania integralności ścieżki audytowej zgodnie z harmonogramami retencji SZBI.

10. Powiązane polityki i zależności

10.1 P1 - Polityka bezpieczeństwa informacji. Ustanawia podstawowe zasady ochrony systemów, danych i sieci. Niniejsza polityka egzekwuje te zasady na poziomie punktów końcowych poprzez techniczne i proceduralne zabezpieczenia przed złośliwym oprogramowaniem.

10.2 P4 - Polityka kontroli dostępu. Określa ograniczenia dostępu użytkowników egzekwowane na poziomie punktów końcowych, w tym zabezpieczenia przed eskalacją uprawnień i nieautoryzowaną instalacją niezweryfikowanego oprogramowania.

10.3 P5 - Polityka zarządzania zmianami. Zapewnia, że aktualizacje oprogramowania ochrony punktów końcowych, reguł polityk lub konfiguracji agentów podlegają zatwierdzeniu i kontrolowanym procesom wdrożeniowym.

10.4 P12 - Polityka zarządzania aktywami. Zapewnia bazową klasyfikację aktywów i inwentaryzację wymaganą do widoczności punktów końcowych, pokrycia wdrażaniem poprawek oraz definiowania zakresu ochrony przed złośliwym oprogramowaniem.

10.5 P22 - Polityka rejestrowania i monitorowania. Umożliwia integrację alertów punktów końcowych, stanu agentów oraz informacji o zagrożeniach ze scentralizowanymi systemami SIEM na potrzeby wykrywania w czasie rzeczywistym i identyfikowalności kryminalistycznej.

10.6 P30 - Polityka reagowania na incydenty (P30). Łączy incydenty złośliwego oprogramowania wykryte na punktach końcowych ze standaryzowanymi procesami w zakresie powstrzymania, usuwania skutków, dochodzenia i odzyskiwania, wraz z przypisanymi rolami i progami eskalacji.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001:

11.1.1 Klauzula 8.1 - Planowanie i nadzór operacyjny: wymaga wdrożenia zabezpieczeń technicznych, w tym zabezpieczeń punktów końcowych, w celu utrzymania celów SZBI.

11.2 ISO/IEC 27002:2022 - Środki kontrolne 8.7, 8:

11.2.1 Zapewnia szczegółowe wytyczne techniczne dotyczące środków ochrony przed złośliwym oprogramowaniem, bezpiecznego wdrażania oprogramowania, monitorowania oraz gotowości do obsługi incydentów w środowiskach punktów końcowych.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Ochrona przed złośliwym kodem: wymaga stosowania narzędzi antymalware z analizą behawioralną oraz skanowaniem w czasie rzeczywistym i przy dostępie.

11.3.2 SI-4 - Monitorowanie systemów: wspiera integrację telemetrii z centralnymi platformami wykrywania.

11.3.3 CM-6 - Ustawienia konfiguracji: wzmacnia bazowe ustawienia kontrolne na punktach końcowych, w tym wymuszanie stosowania agentów ochronnych.

11.4 RODO (2016/679):

11.4.1 Artykuł 32 - Bezpieczeństwo przetwarzania: wymaga od organizacji wdrożenia odpowiednich środków technicznych w celu ochrony danych osobowych, w tym ochrony przed zagrożeniami związanymi ze złośliwym oprogramowaniem.

11.5 Dyrektywa UE NIS2 (2022/2555):

11.5.1 Artykuł 21(2)(d): nakłada na podmioty obowiązek wdrożenia środków wykrywania i zapobiegania zagrożeniom, w tym mechanizmów ochrony przed złośliwym oprogramowaniem na poziomie punktów końcowych.

11.6 Rozporządzenie DORA (2022/2554):

11.6.1 Artykuł 9 - Wymagania dotyczące zarządzania ryzykiem ICT: wymaga, aby podmioty finansowe stosowały środki ochronne zapobiegające zagrożeniom związanym ze złośliwym oprogramowaniem i zagrożeniami przenoszonymi przez punkty końcowe, wykrywające je oraz umożliwiające reagowanie na nie.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Ochrona przed złośliwym oprogramowaniem: wymaga wykrywania i ograniczania skutków złośliwego oprogramowania na wszystkich organizacyjnych punktach końcowych.

11.7.2 DSS01.04 - Zarządzanie dostępnością i wydajnością: zapewnia równowagę pomiędzy ochroną przed złośliwym oprogramowaniem, wydajnością systemów i ciągłością działania.

11.7.3 MEA03 - Monitorowanie, ocena i zapewnienie zgodności: wymaga okresowego audytu zabezpieczeń punktów końcowych i skuteczności ochrony.