Checklista cyberbezpieczeństwa MŚP - 25 punktów

Szybka kontrola podstawowych zabezpieczeń małej lub średniej firmy.

Wersja 1.0	Aktualizacja: 15.09.2026

Konta i dostęp

☐ MFA działa na wszystkich kluczowych kontach.

☐ Hasła są unikalne i przechowywane w menedżerze haseł.

☐ Konta administratorów są oddzielone od codziennych.

☐ Dostępy byłych pracowników są natychmiast blokowane.

☐ Uprawnienia do danych są regularnie przeglądane.

Dane i kopie zapasowe

☐ Najważniejsze dane objęto regularnym backupem.

☐ Jedna kopia jest oddzielona od głównego środowiska.

☐ Odtwarzanie danych jest okresowo testowane.

☐ Dane poufne są szyfrowane w odpowiednich sytuacjach.

☐ Okresy przechowywania danych są określone.

Urządzenia i sieć

☐ Systemy i aplikacje są aktualizowane.

☐ Ochrona endpointów jest aktywna.

☐ Laptopy i telefony mają blokadę ekranu.

☐ Dyski laptopów są szyfrowane.

☐ Router i Wi-Fi mają bezpieczną konfigurację.

Ludzie i procesy

☐ Pracownicy przechodzą szkolenia phishingowe.

☐ Istnieje prosty kanał zgłaszania incydentów.

☐ Dyspozycje finansowe są potwierdzane drugim kanałem.

☐ Zasady pracy zdalnej, chmury i AI są znane.

☐ Onboarding i offboarding obejmują bezpieczeństwo.

Reagowanie i odporność

☐ Firma ma prostą procedurę incydentową.

☐ Istnieje aktualna lista kontaktów awaryjnych.

☐ Zespół zna pierwsze kroki po ransomware.

☐ Firma ma awaryjny sposób pracy bez kluczowego systemu.

☐ Incydenty są dokumentowane i omawiane.

Ważne: Materiał ma charakter edukacyjny i pomocniczy. Nie jest dokumentem prawnym, profesjonalnym audytem ani indywidualną poradą. Dostosuj go do swojej organizacji i rzeczywistego ryzyka.