ALTEM DLA JST • CHECKLISTA 2026

Checklista bezpieczeństwa IT jednostki samorządowej

Praktyczny przegląd kluczowych obszarów bezpieczeństwa i ciągłości działania środowiska IT.

Jak korzystac z materialu?	Zaznacz TAK / NIE / NIE WIEM przy kazdym punkcie. Pozycje NIE i NIE WIEM sa dobrym punktem startu do dalszej analizy. To praktyczna checklista, nie certyfikat zgodnosci ani formalny audyt.

Cel

Checklista pomaga szybko wychwycić obszary, które wymagają weryfikacji. Nie zastępuje formalnego audytu, analizy ryzyka ani oceny zgodności z konkretnymi wymaganiami prawnymi lub sektorowymi.

1. Konta i dostęp

Największym ryzykiem często nie jest sprzęt, ale dostęp użytkowników i administratorów.

01	Każdy użytkownik posiada własne konto, a współdzielone konta są ograniczone do uzasadnionych przypadków.	☐ TAK ☐ NIE ☐ NIE WIEM
02	Konta byłych pracowników i wykonawców są wyłączane według ustalonej procedury.	☐ TAK ☐ NIE ☐ NIE WIEM
03	Dostępy administracyjne są oddzielone od zwykłych kont do codziennej pracy.	☐ TAK ☐ NIE ☐ NIE WIEM
04	MFA jest włączone dla poczty, chmury, VPN i innych kluczowych usług, gdy jest dostępne.	☐ TAK ☐ NIE ☐ NIE WIEM
05	Uprawnienia są okresowo przeglądane i odpowiadają aktualnej roli pracownika.	☐ TAK ☐ NIE ☐ NIE WIEM

2. Stacje robocze i serwery

Aktualność systemów i kontrola konfiguracji ograniczają ryzyko techniczne.

01	Systemy operacyjne i aplikacje otrzymują aktualizacje bezpieczeństwa w przewidywalnym cyklu.	☐ TAK ☐ NIE ☐ NIE WIEM
02	Urządzenia mają aktywną ochronę antymalware / EDR i centralnie monitorowany stan ochrony, jeśli środowisko to umożliwia.	☐ TAK ☐ NIE ☐ NIE WIEM
03	Nieobsługiwane wersje systemów i urządzenia po zakończeniu wsparcia są zidentyfikowane i mają plan wymiany lub izolacji.	☐ TAK ☐ NIE ☐ NIE WIEM
04	Serwery i kluczowe urządzenia są objęte monitoringiem dostępności oraz podstawowych parametrów.	☐ TAK ☐ NIE ☐ NIE WIEM
05	Konfiguracje krytycznych usług są udokumentowane i możliwe do odtworzenia przez więcej niż jedną osobę.	☐ TAK ☐ NIE ☐ NIE WIEM

3. Sieć, dostęp zdalny i segmentacja

Sieć powinna ograniczać skutki pojedynczej awarii lub przejęcia urządzenia.

01	Sieci użytkowników, serwerów, gości, monitoringu CCTV i innych urządzeń są rozdzielone tam, gdzie jest to potrzebne.	☐ TAK ☐ NIE ☐ NIE WIEM
02	Firewall ma aktualne reguły i nie zawiera nieudokumentowanych wyjątków pozostawionych po starych wdrożeniach.	☐ TAK ☐ NIE ☐ NIE WIEM
03	Dostęp zdalny odbywa się kontrolowanym kanałem (np. VPN lub bezpieczna usługa zdalna), a nie przez przypadkowo otwarte porty.	☐ TAK ☐ NIE ☐ NIE WIEM
04	Urządzenia sieciowe mają zmienione domyślne hasła i są objęte aktualizacjami firmware.	☐ TAK ☐ NIE ☐ NIE WIEM
05	Istnieje aktualny schemat sieci, lista urządzeń, adresacji i kluczowych połączeń między lokalizacjami.	☐ TAK ☐ NIE ☐ NIE WIEM

4. Backup i ciągłość działania

Kopia zapasowa ma wartość dopiero wtedy, gdy można z niej odtworzyć działanie.

01	Kopie kluczowych danych i systemów są wykonywane automatycznie według ustalonego harmonogramu.	☐ TAK ☐ NIE ☐ NIE WIEM
02	Co najmniej jedna kopia jest odseparowana logicznie lub fizycznie od środowiska produkcyjnego.	☐ TAK ☐ NIE ☐ NIE WIEM
03	Odtworzenie danych jest okresowo testowane, a wynik testu jest dokumentowany.	☐ TAK ☐ NIE ☐ NIE WIEM
04	Jednostka zna priorytet odtwarzania najważniejszych usług po awarii lub incydencie.	☐ TAK ☐ NIE ☐ NIE WIEM
05	Jest ustalone, kto podejmuje decyzje i kto kontaktuje się z dostawcami w sytuacji poważnej awarii.	☐ TAK ☐ NIE ☐ NIE WIEM

5. Poczta, incydenty i dokumentacja

Bezpieczeństwo wymaga również czytelnych zasad i możliwości odtworzenia historii.

01	Domena pocztowa ma poprawnie skonfigurowane mechanizmy SPF, DKIM i DMARC odpowiednio do używanego systemu pocztowego.	☐ TAK ☐ NIE ☐ NIE WIEM
02	Użytkownicy wiedzą, gdzie zgłosić phishing, podejrzaną wiadomość lub utratę urządzenia.	☐ TAK ☐ NIE ☐ NIE WIEM
03	Incydenty i istotne awarie są rejestrowane w jednym systemie wraz z historią działań.	☐ TAK ☐ NIE ☐ NIE WIEM
04	Dokumentacja infrastruktury jest aktualizowana po zmianach, a nie dopiero przy następnym audycie.	☐ TAK ☐ NIE ☐ NIE WIEM

05	Jednostka potrafi wskazać właścicieli kluczowych usług, wykonawców, numery umów/licencji i dane kontaktowe potrzebne w awarii.	☐ TAK ☐ NIE ☐ NIE WIEM

Najważniejsze braki / kolejne kroki

Chcesz przejść checklistę razem z nami?

Umów bezpłatną konsultację ALTEM dla JST - altem.pl • kontakt@altem.pl